Soft Processing Techniques for Quantum Key Distribution Applications

POLITECNICO DI TORINO

SCUOLA DI DOTTORATO
Dottorato in Elettronica e Comunicazioni – XXIV ciclo

Tesi di Dottorato

Soft Processing Techniques for Quantum Key Distribution Applications

Maria Teresa Delgado Alizo
(160830)

Tutore
prof. Marina MONDIN

Coordinatore del corso di dottorato
prof. Ivo MONTROSSET

12 Marzo 2012

Summary

This thesis deals with soft-information based information reconciliation and data sifting for Quantum Key Distribution (QKD). A novel composite channel model for QKD is identified, which includes both a *hard output* quantum channel and a *soft output* classic channel. The Log-Likelihood Ratios, - also called soft-metrics - derived from the two channels are jointly processed at the receiver, exploiting capacity achieving soft-metric based iteratively decoded block codes. The performance of the proposed mixed-soft-metric algorithms are studied via simulations as a function of the system parameters.

The core ideas of the thesis are employing Forward Error Correction (FEC) coding as opposed to two-way communication for information reconciliation in QKD schemes, exploiting all the available information for data processing at the receiver including information available from the quantum channel, since optimized use of this information can lead to significant performance improvement, and providing a security versus secret-key rate trade-off to the end-user within the context of QKD systems.

Acknowledgments

In anzi tutto desidero ringraziare la prof.ssa Marina Mondin, relatore di questa tesi, per la grande disponibilità e cortesia dimostratemi durante i tre anni di dottorato, e per avermi trasmesso parte della sua passione per la ricerca e l'insegnamento. Ringrazio anche suo marito Fred Daneshgaran, sempre disponibile a chiarire ogni dubbio.

Desidero inoltre ringraziare il prof. Marco Genovese per tutte le discusioni sostenute durante il mio percorso di Dottorato. Della stessa maniera un ringraziamento speciale va a Stefano Olivares per la sua disponibilità e le sue idee che hanno contribuito alla realizzazione di questo lavoro.

Un ringraziamento ai miei colleghi e amici, per essermi stati vicini: Fabio, Antonieta, Miguel (el chino), Ana Paula, Valerio, Alice, Cristina, Vladimir, Laura ed Eduard. Ognuno di voi, in modo diverso, ha contribuito alla mia formazione umana e professionale.

Gracias infinitas a mis padres y hermano por brindarme todo su apoyo y amor durante este y todos los proyectos de mi vida tanto en el plano personal como en el plano profesional. Ustedes son la fuerza que me impulsa, y este, como de costumbre, ha sido un logro compartido. Los quiero mucho familia!

Last but not least, gracias a mi compañero y amigo, Manuel Ignacio Cabrera. Sin ti, todo esto habria sido dificilmente posible y seguramente mucho menos divertido. Te quiero, mi vida.

Table of contents

List of figures

Chapter 1

Introduction

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the shift by 3 rule could decipher his messages.

1.1 Motivation

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography offers among other things confidentiality of data transmissions across insecure networks (like the Internet) and enables the storage of sensitive information so that it cannot be read by anyone except the intended recipient.

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. Encryption is used to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

Before being transmitted, data is encrypted using an encryption algorithm (or process) and a secret key. After transmission, data is decrypted by reversing the encryption algorithm using the same secret key. The security of this scheme is based on the premise that the key is distributed only to the legitimate parties, implying that the key transmission is the central problem.

Today, the ability to ensure the secrecy of military or diplomatic communications is as vital as ever, but cryptography is also becoming more and more important in everyday life. With the growth of computer networks for business transactions and communication of confidential information there is an ever increasing need for encryption to ensure that the information exchanged is secure and cannot be acquired by third parties.

Conventional cryptographic techniques rely on mathematical approaches to secure key transmission. However the security they offer is based on unproven assumptions and depends on the technology available to an eavesdropper.

Quantum Key Distribution is a technology that allows to distribute sequence of random bit whose randomness and secrecy are guaranteed by the laws of quantum physics. These sequences can then be used as secret keys with conventional cryptography techniques to guarantee the confidentiality of data transmissions.

Contrary to what one could expect, the basic principle of quantum key distribution is quite straightforward. It exploits the fact, that according to quantum physics, the mere fact of observing a quantum object perturbs it in an irreparable way. In practice, QKD is combined with conventional key distribution techniques (dual key agreement) to produce a key that is as secure as the strongest of the two original keys. With this approach, one can be sure to get the best of the classical and quantum world. In summary, QKD provides long-term data transmission secrecy, which is not vulnerable to technological progress. On the contrary, classical cryptography provides secrecy only for a limited period of time.

An appropriate question to ask at this point is whether it is possible to actually implement the above quantum key distribution system. The answer is a qualified yes. Up to now, there has been a great interest in experimental QKD, with the current world record distance of 150 km of Telecom fibers[1] and a transmission distance of the quantum bits of 144 km in atmosphere [2], [3]. Although the security of different schemes of quantum key distribution have been studied, modified, improved upon, and even discredit, there is still a tremendous amount of work that needs to be accomplished to create a truly secure and reliable system. Improvements can be made at nearly every level from the actual hardware implementation and software protocols to the actual photon sources and sensitivity of detectors. With the introduction and sale of actual commercial quantum key distribution systems and hardware to be used for secure data transmissions, it is increasingly important that the specifics of quantum key distribution systems are explored and completely characterized.

One such component of a QKD system that requires more scrutiny is the information reconciliation stage. Since the quantum channel of a key distribution system travels along a fairly lossy fiber optic cable or the even more lossy free space medium of the atmosphere, error correction and detection protocols are critical to the proper operation of quantum key distribution. Further, error detection is critical in determining if an eavesdropper is present in the system.

In general, the protocols used for information reconciliation in QKD systems perform error-correction by repeatedly communicating on the public channel and require intense interaction between the parties involved. The same is true for the privacy amplification protocols which are currently considered in the literature [4] and the applications.

1.2 Purpose

The focus of this thesis is on pragmatic information reconciliation and pre-privacy amplification algorithms using novel soft information processing techniques. The proposed techniques can be applied to QKD schemes based both on Single Photon or Weak Laser Pulse (WLP) sources, with or without decoy states[5]. Furthermore, the information reconciliation and pre-privacy amplification algorithms proposed here will mainly use feed-forward techniques, requiring minimal interaction between transmitter and receiver.

More specifically, capacity achieving soft-metric based iteratively decoded block codes will be proposed in order to improve the performance of QKD systems. The availability of soft metric and information bits reliability will be employed to efficiently perform channel probing and pre-privacy amplification.

Soft-information techniques for information reconciliation will be explore in a simulation environment to better ascertain the boundaries of its usefulness, in the detection and correction of errors, during the reconciliation phase of public channel quantum key distribution.

1.3 Outline

This thesis is organized as follows. The first chapter provides a brief background on the concepts necessaries to understand Quantum Key Distribution systems. The basis of classical cryptography are shortly reviewed, followed by a short introduction to quantum mechanics and some ideas from quantum information science useful for QKD systems.

On the second chapter the structure and functioning of a generic QKD protocol is discussed, using as a model one of the most famous protocol invented until now, the BB84 Protocol. In this Chapter particular attention is paid to the Information Reconciliation stage, highlighting the weakness of performing such an important task interactively between sender and receiver.

Third chapter introduces Low Density Parity Check (LDPC) codes, its structure and the advantages of working with capacity achieving codes in the context of practically any communication system, presenting a condensed overview of the belief propagation algorithm used by the LDPC decoders, which is the core of soft-information processing techniques.

In the fourth Chapter, a composite channel model for quantum key distribution is identified, formed by the parallel of the private (quantum) channel and a classic channel. A novel technique for forward error correction based information reconciliation is proposed, exploiting capacity achieving soft-metric based iteratively decoded block codes. The core ideas of this chapter are: a) employing FEC coding as opposed to two-way communication for information reconciliation, minimizing

the interactions between transmitter and receiver; b) exploiting all the available information for data processing at the receiver including information available from the quantum channel; c) using convergence properties of the code to estimate Q_{BER} and presence of an eavesdropper.

Chapter 5 presents the potential improvements in key transmission rate in a Quantum Key Distribution (QKD) scheme whereby photon-counting detectors are used at the receiver. The classical capacity of such system is derived, showing the potential gains that photon counting detectors can provide in the context of a realistic cost-effective scheme from an implementation point of view.

Finally, in the last chapter the simulation results are presented. The performance of the proposed mixed-softmetric algorithms are studied via simulations as a function of the system parameters, in particular the achievable Bit Error Rates(BER) are presented and confronted for different models of the quantum channel. Last a short section will draw the conclusions and the possible further developments of the proposed framework.

Chapter 2

Background

The subject of quantum communications brings together ideas from classical information theory, computer science, and quantum physics. Classical information theory and quantum mechanics fit together very well. In order to explain their relationship, an introduction to classical information theory is given, along with the principles of quantum mechanics. In the next sections a brief overview of classical cryptography and quantum information science is presented, focusing on one of its most important subfields: quantum cryptography.

2.1 Classical Cryptography

Human desire to communicate secretly is at least as old as writing itself and goes back to the beginnings of our civilization. Methods of secret communication were developed by many ancient societies, including those of Mesopotamia, Egypt, India, and China, but details regarding the origins of cryptology[1] remain unknown.

Today, the ability to ensure the secrecy of military or diplomatic communications is as vital as ever, but cryptography is also becoming more and more important in everyday life. With the growth of computer networks for business transactions and communication of confidential information there is an ever increasing need for encryption to ensure that the information exchanged is secure and cannot be acquired by third parties.

Cryptography is the practice and study of encoding and decoding secret messages to ensure secure communications. The main goal is to allow two participants -a sender and an intended recipient- who share no information initially to be able to communicate in a form that is unintelligible to third parties. It is also important to authenticate the messages exchanged to prove that they were not altered during the communication. Both of these goals can be accomplished with provable security if the sender and the recipient are in possession of a shared, secret "key". A key is a

[1] The science of secure communication is called cryptology from Greek *kryptos* hidden and *logos* word. Cryptology embodies cryptography, the art of code-making, and cryptanalysis,the art of code-breaking

piece of information that controls the operation of a cryptographic algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes. Key material, which is a truly random number sequence, is a very valuable commodity even though it conveys no useful information itself. This leads to one of the principal problems of cryptography: the so-called "key distribution problem".

The sender and intended recipient should be able to come into possession of secret key material that third parties "eavesdroppers") cannot acquire, not even partially. It is provably impossible to establish a secret key with conventional communications, so key distribution has relied on the conditional security of "difficult" mathematical problems in public key cryptography.

The search for unbreakable codes is one of the oldest themes of cryptographic research, but until the last century all proposed systems have ultimately been broken.

In 1917, Gilbert S. Vernam proposed an unbreakable cryptosystem, hence called the Vernam cipher or One-time Pad [6]. The One-time Pad is a special case of the substitution cipher[2], where each letter is advanced by a random number of positions in the alphabet. These random numbers then form the cryptographic key that must be shared between the sender and the recipient. Even though the Vernam cipher offers unconditional security against adversaries possessing unlimited computational power and technological abilities, it faces the problem of how to securely distribute the key. In 1949, Shannon proved that the onetime pad is information-theoretically secure, no matter how much computing power is available to the eavesdropper [7]. That is, if the key is truly random, never reused and kept secret, the one-time pad provides perfect secrecy. Note that the one-time pad is the only cryptosystem with perfect secrecy.

Despite Shannon's proof of its security, the one-time pad has serious drawbacks in practice:

- it requires a perfectly random key
- secure generation and exchange of the key must be at least as long as the message.

One time pads require extremely long keys and are therefore prohibitively expensive in most applications. These implementation difficulties have led to one-time pad systems being unpractical and are so serious that they have prevented the one-time pad from being adopted as a widespread tool in information security.

There are two main branches of cryptography: secret (symmetric) key cryptography and public (asymmetric) key cryptography.

[2]The substitution cipher is a well-known classical cipher in which every plaintext character in all its occurrences in a message is replaced by a unique ciphertext character

2.1.1 Public-Key Cryptography

A new surge of interest in cryptography was triggered by the upswing in electronic communications in the late 70s of the 20th century. It was essential to enable secure communication between users who have never met before and share no secret cryptographic key. But the question was how to distribute the key in a secure way. The solution was found by Whitfield Diffie and Martin E. Hellman, who invented public-key cryptography in 1976 [8]. The ease of use of public-key cryptography, in turn, stimulated the boom of electronic commerce during the 1990s.

Public-key cryptography requires two keys: the public key and the private key, which form a key pair. The recipient of a message generates two keys, reveals the public key through a Trusted Authority and keeps his private key in a secret place to ensure its private possession. The algorithm is designed in such a way that anyone can encrypt a message using the public key, however, only the legitimate recipient can decrypt the message using his/her private key.

The security of public-key cryptography rests on various computational problems, which are believed to be intractable. The encryption and decryption algorithms utilize the so-called one-way functions. One-way functions are mathematical functions that are easy to compute in one direction, but their inversion is very difficult. It is, e.g., very easy to multiply two prime numbers, but to factor the product of two large primes is already a difficult task. Other public-key cryptosystems are based, e.g., on the difficulty of the discrete logarithm problem in Abelian groups on elliptic curves or other finite groups. However, it is important to point out that no *one-way function* has been proved to be one-way; they are merely believed to be. Public-key cryptography cannot provide unconditional security.

Today the most widely used public-key system is the RSA cryptosystem. RSA was invented in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman [9], whose names form the acronym. RSA exploits the difficulty of factoring large numbers, it uses a public key N which is the product of two large prime numbers (called "modulus"). Using this key, anyone can encrypt a message. However, in order to invert the algorithm it is necessary to know the prime factors of the modulus.

The possible construction of a quantum computer represents a menace to the security of public-key cryptography. The decryption using a quantum computer would take about the same time as the encryption, thereby making public-key cryptography worthless. Algorithms capable of doing so have already been developed [10] and first experiments with small-scale quantum computers successfully pave the way to more sophisticated devices [11]. For example, one way to crack RSA encryption is by factoring N, but with classical algorithms, factoring becomes increasingly time consuming as N grows large; more specifically, there is not any known classical algorithm that can factor N with a complexity $O((logN)^k)$ for any k. By contrast, Shor's algorithm can crack RSA in polynomial time.

2.1.2 Secret-Key Cryptography

Secret-key cryptography can provide its users with unconditional security on condition that the users share a sufficiently long secret key beforehand. The common key is then used for both encryption and decryption. Secure key distribution is the main drawback of secret-key cryptosystems. The security of communications is reduced to the security of secret-key distribution. In order to avoid the necessity of personal meetings or courier services to exchange the secret key, some users use public-key cryptography to distribute the key, which is then used in a secret-key cryptosystem. The unconditional security of the system is thus degraded to computational security. These so-called hybrid systems have gained a widespread use, because they combine the speed of secret-key systems with the efficiency of key management of public-key systems. They have been used for electronic purchases, financial transactions, ATM transactions and PIN encryptions, identification and authentication of cellular phone conversations, electronic signatures, and many other applications, whose number is swelling.

2.2 Introduction to Quantum Mechanics

Physicists at the end of the nineteenth century believed that most of the fundamental physical laws had been worked out. They expected only minor refinements to get "an extra decimal place" of accuracy. As it turns out, the field of physics was transformed profoundly in the early twentieth century by Einstein's discovery of relativity and by the development of quantum mechanics.

The principles of classical mechanics do not provide the correct description of physical processes if very small length or energy scales are involved. Classical or newtonian mechanics allows a continuous spectrum of energies and allows continuous spatial distribution of matter. In contrast, quantum mechanical distributions are not continuous but discrete with respect to energy, angular momentum, and position. Quantum-mechanics does not contradict newtonian mechanics. As will be seen, quantum mechanics merges with classical mechanics as the energies involved in a physical process increase. In the classical limit, the results obtained with quantum mechanics are identical to the results obtained with classical mechanics. This fact is known as the correspondence principle.

Quantum mechanics (QM), also known as quantum theory, can be formulated according to a few postulates (i.e., theoretical principles based on experimental observations).

2.2.1 Quantum Mechanics Postulates

1. The state of a quantum mechanical system is completely specified by a function $\Psi(\mathbf{r},t)$ that depends on the coordinates of the particle(s) ($\mathbf{r} = (x,y,z)$) and

on time. This function, called the wave function or state function, has the important property that $\Psi^*(\mathbf{r},t)\Psi(\mathbf{r},t)d\tau$ is the probability that the particle lies in the volume element $d\tau$ located at $\mathbf{r}$ at time t The wavefunction must satisfy certain mathematical conditions because of this probabilistic interpretation. For the case of a single particle, the probability of finding it somewhere is 1, so that we have the normalization condition

$$\int_{-\infty}^{\infty} \Psi^*(\mathbf{r},t)\Psi(\mathbf{r},t)d\tau = 1$$

The wavefunction must also be single-valued, continuous, and finite.

2. To every physical observable in classical mechanics there corresponds a linear, Hermitian operator [3] in quantum mechanics. The average value of an observable A represented by an operator $\hat{A}$ for a quantum molecular state $\psi(\mathbf{r})$ is given by the "expectation value" formula

$$< A >= \int \psi^*(\mathbf{r})\hat{A}\psi(\mathbf{r})d\mathbf{r}$$

3. In any measurement of the observable associated with operator $\hat{A}$, the only values that will ever be observed are the eigenvalues a, which satisfy the eigenvalue equation

$$\hat{A}\Psi = a\Psi$$

This postulate captures the central point of quantum mechanics–the values of dynamical variables can be quantized (although it is still possible to have a continuum of eigenvalues in the case of unbound states). If the system is in an eigenstate of $\hat{A}$ with eigenvalue a, then any measurement of the quantity A will yield a. Although measurements must always yield an eigenvalue, the state does not have to be an eigenstate of $\hat{A}$ initially. An arbitrary state can be expanded in the complete set of eigenvectors of $\hat{A}$ ($\hat{A}\Psi_i = a_i\Psi_i$) as

$$\Psi = \sum_i^n c_i\Psi_i$$

where n may go to infinity. In this case we only know that the measurement of A will yield one of the values a_i, but we don't know which one. However, we do know the probability that eigenvalue a_i will occur–it is the absolute value squared of the coefficient, $|c_i|^2$, leading to the fourth postulate below. An important second half of the third postulate is that, after measurement of Ψ yields some eigenvalue a_i, the wavefunction immediately "collapses" into the

[3] See Appendix A

corresponding eigenstate Ψ_i (in the case that a_i is degenerate, then Ψ becomes the projection of Ψ onto the degenerate subspace). Thus, measurement affects the state of the system. This fact is used in many elaborate experimental tests of quantum mechanics.

4. If a system is in a state described by a normalized wave function Ψ, then the average value of the observable corresponding to $\hat{A}$ is given by

$$< A >= \int_{-\infty}^{\infty} \Psi^* \hat{A} \Psi d\tau$$

5. The wavefunction or state function of a system evolves in time according to the time-dependent Schrödinger equation

$$\hat{H}\Psi(\mathbf{r},t) = i\hbar \frac{\partial \Psi}{\partial t}$$

2.2.2 Bra-Ket Notation

In quantum mechanics, since wavefunctions can be added in linear combinations just like vectors,

$$\Psi = \sum_n c_n \phi_n$$

Paul Dirac [12] created a powerful and concise formalism for quantum mechanics, which is now referred to as Dirac notation, or Bra-Ket notation $\langle bra|c|ket\rangle$ notation.

Dirac introduced a notation to:

1. Extend the idea of multiple spatial basis sets (such as above) to incorporate the state of the system into the a basis set. Momentum components, energy levels, quantum numbers, spins, can be thought of as basis vectors for a wavefunction in the Hilbert space (in this instance a simple, real-valued Euclidean vector space is insufficient). Hence the basis vectors indicate the state of the system, and the state of a physical system is identified with a ray in a complex separable Hilbert space, $\mathcal{H}$, or, equivalently, by a point in the projective Hilbert space of the system. Each vector in the ray a ket written as $|\psi\rangle$.

2. Use any useful set of basis vectors to construct the overall quantum state: the wavefunction as a vector in the vector space, rather than a mathematical function. Since any basis can be used, the wavefunction is basis-independent.

A quantum state is then represented by the ket $|\psi\rangle$. The Hermitian conjugate is the bra $\langle\psi|$, and the inner product is

$$\langle\psi|\phi\rangle = c(a\ number)$$

If $c = \langle\psi|\phi\rangle$ then the complex conjugate is $c^* = \langle\psi|\phi\rangle^* = \langle\phi|\psi\rangle$. For more information on the Dirac notation please refer to the appendix A.

2.3 Quantum Information Science

Quantum information science (QIS) is a new field of science and technology, that combines several disciplines such as physical science, mathematics, computer science, and engineering. Its aim is to understand how certain fundamental laws of physics discovered earlier in this century can be harnessed to dramatically improve the acquisition, transmission, and processing of information.

The field of QIS had an explosive growth in the early to mid 1990s as a consequence of several simultaneous stimuli: Peter Shor demonstrated that a quantum computer could factor very large numbers super-efficiently [10] and the semiconductor industry realized that the improvement of computers according to Moore's law would all too soon reach the quantum limit[13], requiring radical changes in technology. Developments in the physical sciences produced advances that made it possible to contemplate the construction of workable quantum logic devices. Furthermore, the need for secure communications drove the investigations of quantum communication schemes that would be tamper proof.
In the past decades the miniaturization of electronic circuitry on silicon chips has shown steady advances, allowing performance to double roughly every 18 months ("Moore's law"). At this rate, in less than 20 years, this shrinkage will reach atomic dimensions. It is known that atoms and other tiny particles obey laws of quantum physics that in many respects defy common sense. For example, observing an atom disturbs its motion, while not observing it causes it to spread out and behave as if it were in several different places at the same time. Until recently such quantum effects have mostly been seen as a nuisance, causing small devices to be less reliable and more error-prone than their larger cousins.

In classical information theory, the basic unit of information is the *bit* or binary digit, that can only assume one of two possible distinct states.In quantum computing, the unit of quantum information is known as a *qubit* or a quantum bit.

Consider the binary strings,

$$\{000\}\{001\}\{010\}\{011\}\{100\}\{101\}\{110\}\{111\}$$

The first one can represent, for example, the number 0 (in binary), the second one the number 1, the third one the number 2 and so on. In general three physical bits can be represented in $2^3 = 8$ different configurations, that correspond to the integers from 0 to 7. However, a register composed of three classical bits can store only one number at a given moment of time.

2.3.1 The qubit

A qubit is a quantum system in which the Boolean states 0 and 1 are represented by a prescribed pair of normalized and mutually orthogonal quantum states labeled as $\{|0\rangle,|1\rangle\}$ [4].

The two states form a 'computational basis' and any other (pure) state of the qubit can be written as a superposition $\alpha|0\rangle + \beta|1\rangle$ where α and β are probability amplitudes and can in general both be complex numbers, such that $\alpha^2 + \beta^2 = 1$.

The probability that the qubit will be measured in the state $|0\rangle$ is $|\alpha|^2$ and the probability that it will be measured in the state $|1\rangle$ is $|\beta|^2$. Hence the total probability of the system being observed in either state $|0\rangle$ or $|1\rangle$ is "1", this situation been significantly different from the state of a classical bit, which can only take the value 0 or 1.

Thus, the main difference between a bit and a qubit is that whereas a bit must be either 0 or 1, a qubit can be 0, 1, or a *superposition* of both. A qubit can be described by a quantum state in a two-state quantum-mechanical system, which is formally equivalent to a two-dimensional vector space over the complex numbers; is typically a microscopic system, such as an atom, a nuclear spin, or a polarized photon.

2.3.2 Bloch Sphere

In quantum mechanics, the Bloch sphere (also known as the Poincar sphere in optics) is a geometrical representation of the pure state space of a 2-level quantum system. Alternatively, it is the pure state space of a 1 qubit quantum register. The Bloch sphere is actually geometrically a sphere and the correspondence between elements of the Bloch sphere and pure states can be explicitly given.

To show this correspondence, consider the qubit description of the Bloch sphere; any pure state Ψ can be written as a complex superposition of the ket vectors $|0\rangle$ and $|1\rangle$; moreover since global phase factors do not affect physical state, we can take the representation so that the coefficient of $|0\rangle$ is real and non-negative. Thus Ψ has a representation:

$$|\psi\rangle = \cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle$$

with

$$-\frac{\pi}{2} \leq \theta < \frac{\pi}{2}, \quad 0 \leq \varphi < 2\pi.$$

The representation is unique except in the case Ψ is one of the ket vectors $|0\rangle$ or $|1\rangle$ The parameters ϕ and θ uniquely specify a point on the unit sphere of euclidean

[4] The term was coined by B. Schumacher. See, Phys. Rev. A 51 2738 (1995)

space $\mathbb{R}^3$, namely the point whose coordinates (x,y,z) are

$$\begin{aligned} x &= \sin 2\theta \times \cos\varphi \\ y &= \sin 2\theta \times \sin\varphi \\ z &= \cos 2\theta \end{aligned}$$

In this representation $|0\rangle$ is mapped into (0,0,1) and $|1\rangle$ is mapped into $(0,0,-1)$.

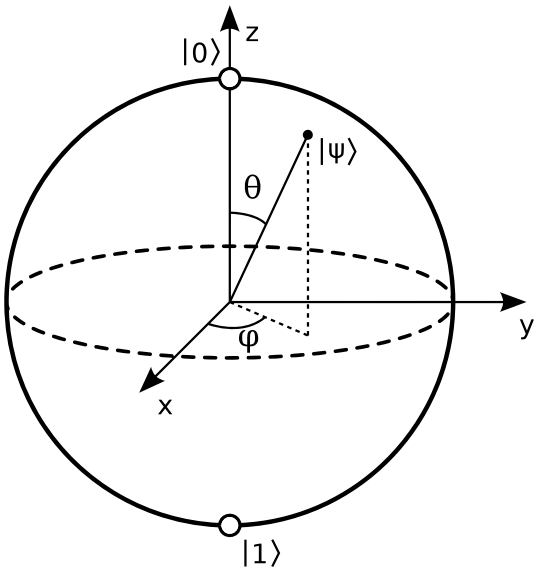


Figure 2.1: Bloch Sphere

The interior of the Bloch sphere, the open Bloch ball, represents the mixed states of a single qubit. The $\vec{r} = (x,y,z)$ co-ordinates of a state represent the expectation values of the $\sigma(x,y,z)$ operators respectively. This is conveniently expressed by,

$$\rho = \frac{1}{2}(\mathbb{I} + \vec{r} \cdot \vec{\sigma})$$

where $\mathbb{I}$ is the 2x2 identity matrix, and $\vec{r}.\vec{\sigma} = \sum_{j=x,y,z} r_j \sigma_j$.

A convex combination of pure states $\{\hat{\vec{r}}_j\}$ with weights p_j gives a mixed state with Bloch vector $\vec{r} = \sum_j p_j \hat{\vec{r}}_j$.

2.3.3 Pure and mixed states

A pure quantum state is a state which can be described by a single ket vector, or as a sum of basis states. A mixed quantum state is a statistical distribution of pure states.

The expectation value ⟨a⟩ of a measurement A on a pure quantum state is given by

$$\langle a\rangle = \langle\psi|\hat{A}|\psi\rangle = \sum_i a_i\langle\psi|\alpha_i\rangle\langle\alpha_i|\psi\rangle = \sum_i a_i|\langle\alpha_i|\psi\rangle|^2 = \sum_i a_i P(\alpha_i)$$

where $|\alpha_i\rangle$ are basis kets for the operator $\hat{A}$, and $p(\alpha_i)$ is the probability of $|\psi\rangle$ being measured in state $|\alpha_i\rangle$.

In order to describe a statistical distribution of pure states, or mixed state, the density operator (or density matrix), ρ, is used. This extends quantum mechanics to quantum statistical mechanics. The density operator is defined as

$$\rho = \sum_s p_s|\psi_s\rangle\langle\psi_s|$$

where ps is the fraction of each ensemble in pure state $|\psi_s\rangle$. The ensemble average of a measurement A on a mixed state is given by

$$\langle\overline{A}\rangle = \sum_s p_s\langle\psi_s|A|\psi_s\rangle = \sum_s\sum_i p_s a_i|\langle\alpha_i|\psi_s\rangle|^2 = tr(\rho A)$$

where it is important to note that two types of averaging are occurring, one being a quantum average over the basis kets of the pure states, and the other being a statistical average over the ensemble of pure states.

Operations on pure qubit states

There are various kinds of physical operations that can be performed on pure qubit states.

1. *Quantum logic gates*, that can operate on a qubit: mathematically speaking, the qubit undergoes a unitary transformation. Unitary transformations correspond to rotations of the Bloch sphere.
2. *Standard basis measurement* which is an operation where information is gained about the state of the qubit. The result of the measurement will be either $|0\rangle$, with probability α^2, or $|1\rangle$, with probability β^2. Measurement of the state of the qubit alters the values of α and β. For instance, if the result of the measurement is $|0\rangle$, α is changed to 1 (up to phase) and β is changed to 0.

Ensemble

An ensemble of quantum states is a set of quantum states with corresponding probabilities. An ensemble $\mathcal{E}$ is written

$$\mathcal{E} = \{(p_i,\rho_i)\},$$

where pi is the probability for the state p_i.

To each ensemble there is a corresponding average state

$$\bar{\rho} = \sum_i p_i \rho_i,$$

but any mixed state can be realized by many different ensembles, even if the states in the ensemble are restricted to pure states.

Usage

1. For sending classical information over quantum channels, one has to choose an ensemble of states to encode the information. The maximum information which is possible to transmit with a given ensemble is called the accessible information.
2. A (non-destructive) measurement on a quantum state will define an ensemble of post-measurement states. If the measurement outcome is discarded, the state will be in the average state.
3. Different ensembles of pure states is used to define the entanglement of formation.

2.3.4 Quantum Mechanics Interpretation

In the previous section a brief introduction to the postulates of quantum mechanics has been given. It has been said that these postulates cannot be proven or deduced. They are hypotheses, and, if no violation with nature (experiments) is found, they are called axioms, i. e. non-provable, true statements. The five postulates are a concise summary of the principles or quantum mechanics. They have severe implications on the interpretation of microscopic physical processes, while on a macroscopic scale, quantum-mechanics smoothly merges into newtonian mechanics for any physical process. Next, some considerations are presented, aiming to illustrate the implications of the QM postulates:

- *A measurement cannot be perform without perturbing the system.* Furthermore, there is no avoiding the rather dramatic effect that the measurement has on the system the reduction of the wave function to one of the eigenfunctions of the measurement operator.
- *The values of two quantities cannot be simultaneously known with certainty if the corresponding operators do not commute.* Assume that the state of the system is described by an eigenfunction $u_k(x)$ of the measurement operator $\hat{A}$, at the time of the measurement. In this case, we can predict with certainty that the outcome of the measurements will be the corresponding eigenvalue, a_k. In

order to simultaneously know the value of another observable quantity represented by $\hat{B}$, with certainty, also has to be an eigenfunction of $u_k(x)$. However, we have found before that two hermitian operators can share a complete set of eigenfunctions if and only if they commute, i.e. if . $[\hat{A},\hat{B}] = 0$ [5]

- *The creation of identical copies of an arbitrary unknown quantum state is forbidden.* This is due to the fact that all quantum operations must be unitary linear transformation on the state.[6]

All of these principles have found profound implications in quantum information science and many of it subfields, with many applications in the modern world. Among the subfields of QIS, one of the most important is quantum cryptography (QC) [16], QC has emerged as one of the most relevant practical applications of quantum theory. While the security of the traditional cryptographic techniques is based on algorithmic complexity of solving certain mathematical problems (e.g., one-way functions), the security of quantum cryptography is founded on quantum physical principles. As a consequence, quantum mechanics is able to generate *perfectly secure* random keys that can then be used in standard secret-key protocols. This will discussed further in detail in Chapter 3.

[5] This is also known as the Heisenberger's Uncertainty Principle[14]
[6] No-cloning theorem[15]

Chapter 3

Quantum Cryptography

3.1 Motivation

It has been said that the security of conventional cryptographical techniques relies on the assumption of limited advancement of mathematical algorithms and computational power in the foreseeable future, and also on limited financial resources available to a potential adversary. Computationally secure cryptosystems, no matter whether public- or secret-key, will always be threatened by breakthroughs, which are difficult to predict, and even steady progress of code-breaking allows the adversary to reach back in time and break older, earlier captured, communications encrypted with weaker keys. As a consequence, the necessity to periodically re-encrypt or re-sign certain documents is necessary, along with the requirement to carefully sort information according to the used cryptosystem. Besides this, another common problem of conventional cryptographic methods is the so-called side-channel cryptanalysis. Side channels are undesirable ways through which information related to the activity of the cryptographic device can leak out. The attacks based on side-channel information do not assault the mathematical structure of cryptosystems, but their particular implementations. It is possible to gain information by measuring the amount of time needed to perform some operation, by measuring power consumption, heat radiation or electromagnetic emanation.

Quantum mechanics offers a solution for the secure key distribution in cryptosystems. While the security of classical cryptographic methods can be undermined by advances in technology and mathematical algorithms, the quantum approach can provide *unconditional security*. In quantum mechanics the security is guaranteed by the *Heisenberg uncertainty principle*, which does not allow us to discriminate nonorthogonal states with certainty. Within the framework of classical physics, it is impossible to reveal possible eavesdropping, because information encoded into any property of a classical object can be obtained without affecting the object itself. All classical signals can be monitored passively. In classical communications, one bit of information is encoded in billions of photons, electrons, atoms or other carriers. It is

always possible to passively listen in, by splitting part of the signal and performing a measurement on it. Quantum cryptosystems eliminate this side channel by encoding each bit of information into an individual quantum object, such as a single photon. Single photons cannot be split, copied or amplified without introducing detectable disturbances.

It is important to notice that quantum mechanics does not prevent from eavesdropping; it only allows to detect the presence of a possible eavesdropper. Since only the cryptographic key is transmitted, no information leak can take place when someone attempts to listen in. When discrepancies are found, the key is simply discarded and the users may repeat the procedure to generate a new key.

3.2 Quantum Key Distribution

In the early 1980s, Bennett and Brassard proposed a solution to the key distribution problem based on quantum physics [17], they presented a protocol that allows users to establish an identical and purely random sequence of bits at two different locations, while allowing to reveal any eavesdropping with a very high probability. This idea, independently rediscovered by Ekert a few years later [18], was the beginning of quantum key distribution, which was to become the most promising task of quantum cryptography[1].

Quantum Key Distribution (QKD)is a technology to distribute, or rather generate, secure random keys between two communicating parties using optical fiber or free-space as a communication channel. It has been said that QKD has emerged in the last decades as one of the most important applications of quantum mechanics. Hence, in this section the basic configuration and elements of such an important application will be introduced. Alternative introductions to this subject are available in many sources, ranging from books [19],[20],[21],[22] to other review articles [16],[23],[24].

3.2.1 Generalities

The general settings of QKD are shown in 3.1. The two *authorized partners*, are traditionally called Alice and Bob. *Alice*, the sender, is the one who starts a key transmission, while *Bob*, the receiver, is the one who receives the quantum states and extracts the key sent by Alice. This is just a convention used in the field, but not a strict definition. The third important character is the eavesdropper, *Eve*, who is trying to intrude into the QKD and gain information about the key generated between Alice and Bob. Alice and Bob share a quantum *secure* channel, on which

[1]For some authors, quantum cryptography and quantum key distribution are synonymous. For others, however, quantum cryptography also includes other applications of quantum mechanics related to cryptography, such as quantum secret sharing or every other possible tasks related to secrecy that are implemented with the help of quantum physics

they send the *quantum* signals; and a classical public channel, on which they can send classical messages forth and back. The classical channel needs to be authenticated: this means that Alice and Bob identify themselves; a third party can listen to the conversation but cannot participate in it. The quantum channel, however, is open to any possible manipulation. The task of Alice and Bob is that of guaranteing security against a possible eavesdropper that taps into the quantum channel and listen to the exchanges on the classical channel. In order to guarantee the security, either the authorized partners are able to create a secret key (a common list of secret bits known only to themselves) or they shall abort the protocol. Therefore, after the transmission of a sequence of symbols, Alice and Bob must estimate how much information about their set of bits has leaked out to Eve. In classical communications, such an estimate is obviously impossible, when Eve listens to the exchanges on the classical channel the communication goes on unmodified. This is where quantum physics comes into the game: in a quantum channel, the leak of information is directly related to the degradation of the communication quality.

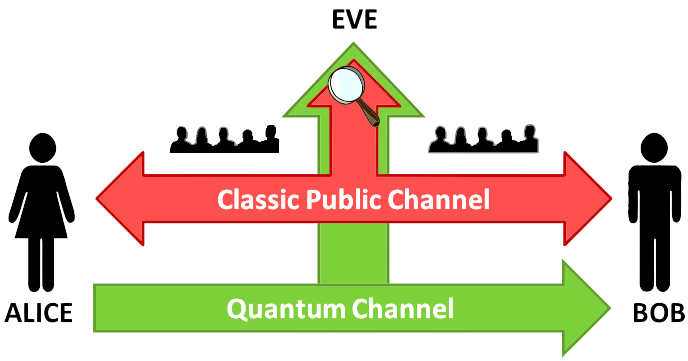


Figure 3.1: Quantum key distribution comprises a quantum channel and a public classical authenticated channel. As a universal convention in quantum cryptography, *Alice* sends quantum states to *Bob* through a quantum channel. *Eve* is suspected of eavesdropping on the line.

The choice of light

In general, quantum information processing can be implemented with ions, atoms, light, spins, etc. Abstractly, this is the case also for QKD: one could imagine performing a QKD experiment with electrons, ions, and molecules; however, light is the only practical choice. Indeed, the task of key distribution makes sense only if Alice and Bob are separated by a macroscopic distance: if they are in the same room, they have much easier ways of generating a common secret key. Since, at a determinate distance, light propagates faster and with smaller decoherence than matter, photons are the information carriers by excellence. Various properties of photons can be employed to encode information for QKD, such as polarization, phase, quantum correlations of Einstein-Podolsky-Rosen pairs, wavelength or quadrature components of

squeezed states of light.

It is known that light does not interact easily with matter. The way losses affect QKD varies with the type of protocol and its implementation. Losses impose bounds on the secret key rate and on the achievable distance and may also leak information to the eavesdropper, according to the nature of the quantum signal (for coherent pulses this is certainly the case while for single photons it is not). Another difference is determined by the detection scheme. Implementations that use photon counters rely on post-selection: if a photon does not arrive, the detector does not click and the event is simply discarded; on the contrary, implementations that use homodyne detection always give a signal, therefore losses translate as additional noise. QKD is always implemented with light and there is no reason to believe that things will change in the future. As a consequence, the quantum channel is any medium that propagates light with reasonable losses, typically either an optical fiber or just free space, provided a line of sight path exists between Alice and Bob.

3.2.2 The BB84 Protocol

In order to understand all of the concepts presented before -and some others that will be introduced later-, in this section the basic ideas of QKD will be described using a very concrete example: the BB84 protocol. Suppose Alice holds a source of single photons. The spectral properties of the photons are sharply defined, so that the only degree of freedom left is the polarization[2].

Alice and Bob align their polarizers[3] and agree to use either the horizontal or vertical (+) basis (*rectilinear*), or the complementary basis of linear polarizations, i.e., +45/-45 (×) (*diagonal*). Specifically, the bits are encoded as follows:

$$\begin{array}{ll} |H\rangle \longrightarrow 0_+ & |+45\rangle \longrightarrow 0_\times \\ |V\rangle \longrightarrow 1_+ & |-45\rangle \longrightarrow 1_\times \end{array}$$

where both bit values 0 and 1, are encoded in two possible ways in *non-orthogonal* states, since $|\pm 45\rangle = \sqrt{2}/2(|H\rangle \pm |V\rangle)$

It is important to notice that these four states satisfy the following relations:

$$\langle H|V\rangle = \langle -45| + 45\rangle = 0 \tag{3.1}$$

$$\langle H|H\rangle = \langle V|V\rangle = \langle +45| + 45\rangle = \langle -45| - 45\rangle = 1 \tag{3.2}$$

$$|\langle H| \pm 45\rangle|^2 = |\langle V| \pm 45\rangle|^2 = 1/2 \tag{3.3}$$

Interpretation:

- Measurements performed in the basis identical to the basis of preparation of states will produce deterministic results (eq. 3.1 and 3.2)

[2]Usually the way to encode the information being sent over the quantum channel is through the transmission of photons in some polarization states. The direction of the polarization encodes a classical bit.

[3]A polarizer is an optical filter that passes light of a specific polarization and blocks waves of other polarizations

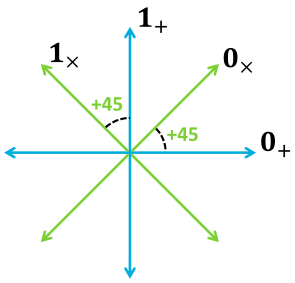


Figure 3.2: The four states of the BB84 Protocol

- Any measurements in the diagonal basis on photons prepared in the rectilinear basis will yield random outcomes with equal probabilities and viceversa (eq. 3.3)

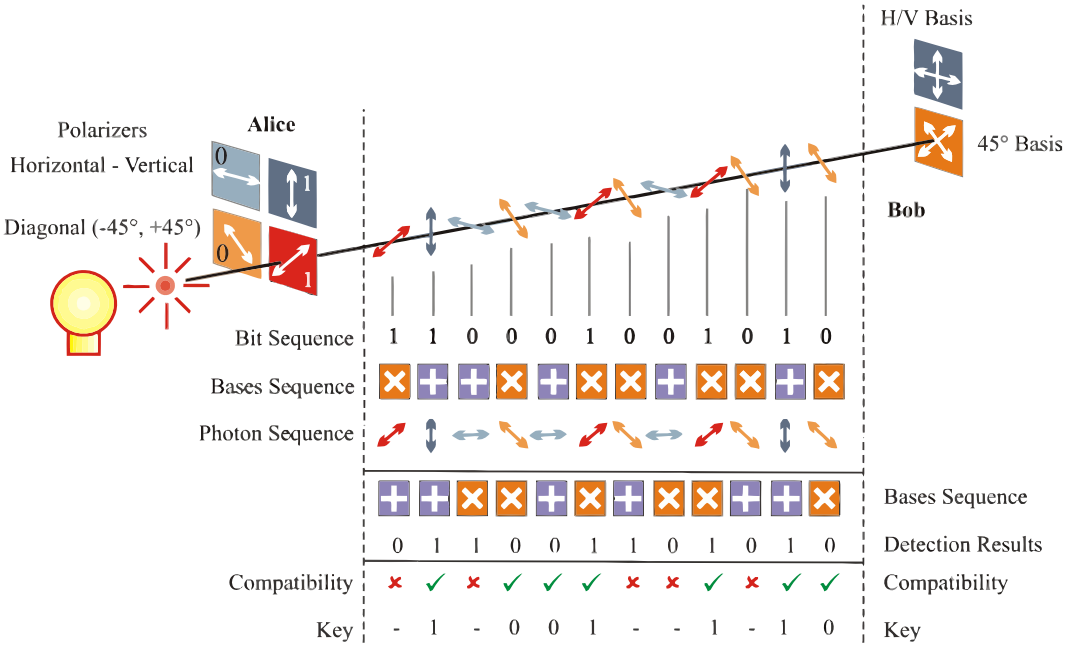


Figure 3.3: BB84 Protocol

Once Alice and Bob have agreed on the coding, the BB84 protocol can be summarize in the following steps:

1. **Key Transmission** Alice, the sender, generates a sequence of N random bits for transmission and chooses the encoding basis (rectilinear or diagonal) in a random and independent way for each bit. Physically it means that she transmits photons in the four polarization states $|H\rangle$,$|V\rangle$,$|+45\rangle$,$|-45\rangle$ with equally

distributed frequencies. Bob, the receiver, randomly and independently of Alice, chooses his measurement basis, either rectilinear or diagonal. Statistically, their bases match in 50% of the cases. At the end of this stage Alice and Bob will share what is called the ***raw key***

2. **Basis Announcement** Alice and Bob communicate over the classical channel and compare the basis used for each transmitted and detected photon. Whenever their bases coincide, Alice and Bob keep the bit whereupon it becomes part of the cryptographic key. The bit is discarded when they chose different basis, when Bob's detector failed to register a photon -due to the imperfect efficiency of detectors-, or when the photon was lost somewhere on the way. Any potential eavesdropper, can only learn if Alice and Bob chose the same basis, but cannot determine whether Alice originally sent a "0″ or "1″. This step is called ***sifting***. At the end, Alice and Bob have a string of bits of approximately N/2 bits, called the ***sifted key***

3. **Error Estimation** Alice and Bob disclose part of their strings -a subset of positions of size K- and estimate the error rate in the quantum channel.

   As shown in Chapter 2, if Eve tries to eavesdrop on the quantum channel, she cannot passively monitor the transmissions. Instead she can intercept the photons sent by Alice, perform measurements on them and resend them. However, since Alice had chosen her encoding bases randomly Eve has to guess. Half the times Eve will guess the basis right and resend correctly polarized photons, while in the other 50% of the cases, she measures in the wrong basis, producing errors.

   When Alice and Bob reveal a random sample of the bits of their raw keys, they discover these errors. Alice and Bob use a predetermined "failure" error threshold (e_{max}) to decide whether or not an eavesdropper is present. In the literature, the most common failure error rate chosen is greater than or equal to 0.15 [25]. At 0.15 error rate, an eavesdropper could have intercepted over half of the bits transmitted.

   Both players compute the observed error-rate e and accept the quantum transmission if $e \leqslant e_{max}$, set initially by Alice, in this case they remove the K bits announced from the raw key. Otherwise if $e > e_{max}$ eve is suspected of tampering with the channel, and the cryptographic key is thrown away. Thus, no information leak occurs even in the case of eavesdropping. It should be mentioned that no physical apparatus is perfect and noiseless. Alice and Bob will always find discrepancies, even in the absence of Eve. As they cannot tell errors stemming from eavesdropping from the noise of the apparatus, they conservatively attribute all the errors in transmissions to Eve. The actual error rate stems from both noise in the channel and possibly, interference from an eavesdropper.

4. **Reconciliation and Privacy Amplification** If there are errors, however, Alice and Bob have to correct them and have to eliminate the information that could have been obtained by Eve[4].

   Information reconciliation is a form of error correction carried out between Alice and Bob's keys, in order to ensure both keys are identical. It is conducted over the public channel and as such it is vital to minimize the information sent about each key, as this can be listen by Eve. Alice and Bob perform the error correction through an interactive reconciliation protocol called *Cascade*. This is a simple protocol that leaks an amount of information close to the theoretical bound of an *almost ideal* protocol[5], when the error probability is below 15%. *Cascade* was presented in [26] as an improvement of the procedure suggested in [27].

   Cascade operates in several rounds. During each round, Alice and Bob divide their raw keys into blocks, and disclose the parity of each block and compare them. If the parity bits do not match then a *binary* search is performed in order to find and correct the error. After all blocks have been compared, Alice and Bob both reorder their keys in the same random way, and a new round begins. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is found and corrected as before. This process is repeated recursively, which is the source of the cascade name. At the end of multiple rounds Alice and Bob have identical keys with high probability, however Eve has additional information about the key from the parity information exchanged. Once the information reconciliation has been performed, Alice and Bob share what is known as the ***reconciled key***.

   Privacy amplification is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key. This partial information could have been gained both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors), and on the public channel during information reconciliation (where it is assumed Eve gains all possible parity information). Privacy amplification uses Alice and Bob's key to produce a new, condensed key, in such a way that Eve has only negligible information about the new key. This can be done using universal hashing functions, chosen randomly from a publicly known set. The size r of the ***secret key*** that Alice and Bob can distill depends on the kind -as well as the amount- of information available to Eve.

In figure 3.3 a very simplified scheme of the BB84 protocol is shown. At the first stage, Alice chooses randomly the basis to encode the polarization of the photons

[4]Historical note: the procedure that erases the information obtained by the eavesdropper was not discussed by Bennett and Brassard (1984) and first appeared a few years later (Bennett, Brassard, and Robert, 1988).

[5]Brassard and Salvail have formulated some definitions to characterize reconciliation protocols in [26]

that she sends through the quantum channel. Bob, as well, chooses randomly the basis to decode the photon's polarization. Then they exchange some information on the public channel and keep only the bits they have encoded/decoded with the same basis and throw away the rest, generating what has been called the "sifted key".

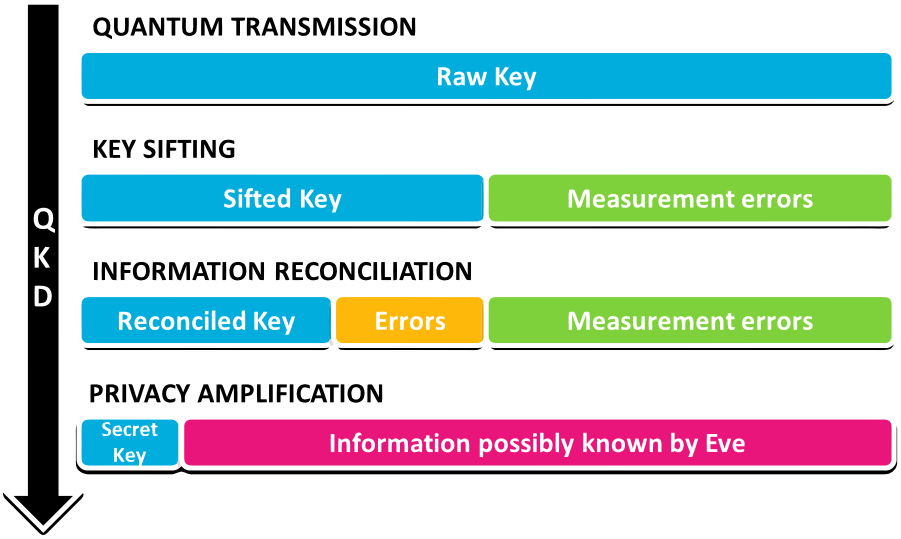


Figure 3.4: Distillation process and key length in BB84 Protocol

In a very general way, the steps of any QKD protocol can be resume as follows:

1. Key Exchange→ The qubits are exchanged between the two parties over the quantum channel. It leads to the generation of the raw key.

2. Key Sifting→ The basis are announced. After the sifting step, both parties share the sifted key.

3. Key Distillation→ After sifting, the emitter and the receiver jointly process the sifted key to distill a secure sequence of bits called the secret key. The process consists itself of three steps:

   (a) Error correction

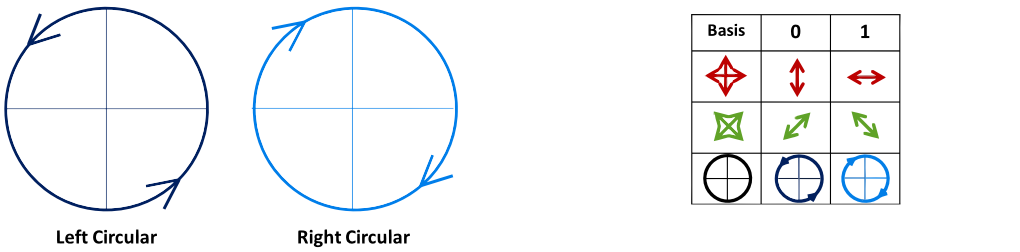
   (b) Privacy amplification

   (c) Authentication

In figure 3.4 the distillation process of the secret is presented. It is important to notice that the final distilled key has a very short length when compared to the initial key size.

3.2.3 Information Reconciliation

In order to preserve the integrity and security of their keys, Alice and Bob utilize an interactive reconciliation protocol called Cascade, which consists of two-way interactions between Alice and Bob over a public classical channel for the detection and correction of errors, where many messages are openly passed back and forth. The Cascade error reconciliation protocol is actually a modification of an earlier protocol *BBBSS*, proposed by Bennett et al. in 1991 [27]. BBBSS utilized an interactive error detection and correction protocol that the authors called *Binary*. BBBSS used a modified BB84 QKD protocol using a circular polarization basis instead of the diagonal basis. Other than the basis substitution, BBBSS operated as a BB84 implementation.



(a) Circular Basis

(b) Basis used in BB84 and BBBSS protocols

Figure 3.5: Basis for QKD Protocols

The procedure described in [27] for Alice and Bob to reconcile their bits takes place over a public channel. Since Eve presumably listens to all public transmissions, Alice and Bob must reveal as little information as possible while still ensuring that they end up with identical keys.

If the estimated error rate in the sifted key is acceptable, Alice and Bob begin the first of a number of passes, and use a predetermined random permutation, that is applied to the key bits. The purpose of the permutation is to attempt to spread out the error bits randomly and separate consecutive errors from each other.

- Alice and Bob then divide all of the sifted key bits into blocks of N bits dependent upon the estimated error rate with the goal of having one or fewer errors remaining per block.
- Alice and Bob then use the classical channel to compare block parities. For blocks where the parities disagree, there must be an odd number of errors since an even number of errors would mask each other. The block is then divided in half, into two smaller blocks of length, and another parity check is conducted on the first sub-block. Since there is definitely at least one error in one of the sub-blocks, the parity of one sub-block reveals where the error has occurred.

The sub-block with the error is further sub-divided and parity checked until the error bit is found. The error is then corrected.

- Since the exchange of parity bits occurs on the classical channel, over which Eve can passively eavesdrop, it is assumed that the parity bits give Eve information about the secret key. By discarding the last bit of each block and sub-block involved in a parity check, the information that Eve gains about the key can be reduced.
- Since a number of even errors cannot be detected, the key is then permuted again and the Binary search check protocol is run again. In order to reduce the amount of discarded bits wasted when a parity check passes, essentially a lost potential key bit, the Binary protocol utilizes an additional process during later passes that wastes fewer bits. The authors refer to the new mode as *confirm and bisect*. In this stage, the parity of a random subset of the sifted key is calculated and compared. Subsets that fail the parity check are subdivided and checked using Binary.

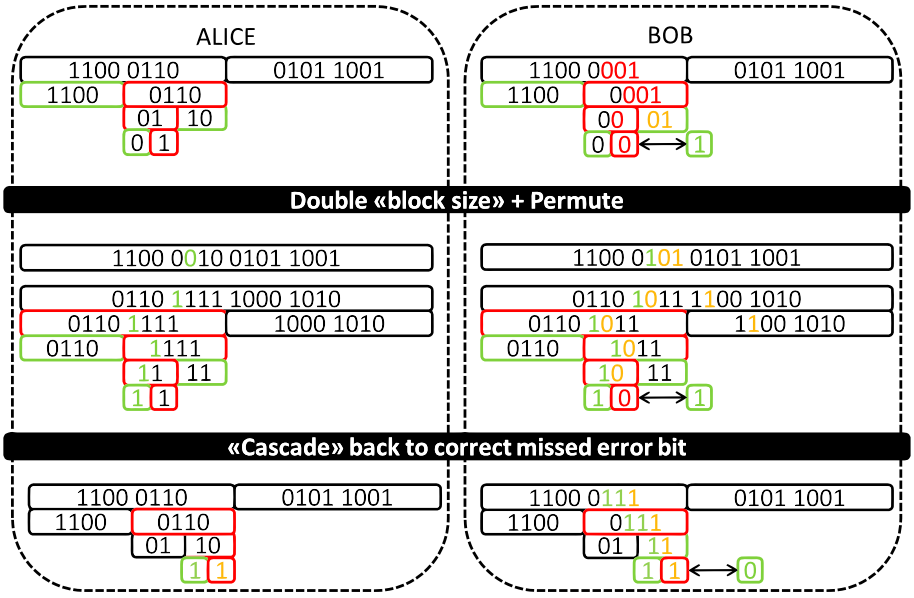


Figure 3.6: Cascade Protocol. The colored numbers represent the error bits (red) and the masked error bits (orange), while colored borders represent failed (red) or passed (green) parity checks

Brassard and Salvail created the Cascade reconciliation protocol as an improvement to Binary in terms of bits leaked during the reconciliation stage [26]. By increasing the processing steps of the protocol, the authors claimed to have improved upon the information leakage problem and reduced bits leaked to the theoretical minimum needed to perform reconciliation. The operation of Cascade is nearly

identical to Binary except that the error bit locations and values are retained for use in later passes, so the algorithm can correct all odd number errors and then cascade back through the previous passes to find even errors that were previously masked. A detailed description of the operation of Cascade is given below.

- Cascade protocol begins with an estimated error rate analysis of the sifted keys. The analysis is conducted as in BBBSS, with a subset of the sifted key compared across the classical channel between Alice and Bob.
- Alice and Bob divide their sifted keys into blocks with a size dependent upon the error rate.
- The block parities are compared between Alice and Bob over the public channel, and Binary is used to correct errors. The final bit of each block involved is not discarded at this point. In addition, all of the information regarding error location is stored.
- After a permutation of the sifted key, a new pass is started. However, unlike in BBBSS, the block size is increased and another Binary search is conducted. Any errors found in this pass could only have resulted from two or more even number of errors that were masking each other in the previous pass. Using the information on error location stored from the previous pass, the Cascade algorithm returns to the shortest block that involved the initially corrected error from pass 1 and bisect it to find the hidden error.

The protocol proceeds to operate in the same way with all discovered errors, cascading through previous passes to find and correct masked bits. After a number of passes, permutations, and cascades, the protocol finishes with low probability that errors still remain.

3.2.4 The Problem

In practice, there are several problems with the protocols presented in the previous sections. The first one, is that real photon detectors always have some noise, so even without eavesdropping, Alice and Bob's bits will differ. Secondly, current technology is not good enough to reliably generate single photons. Actual photon emitters can generate pulses of light with a given average number, m, of photons per pulse, but not necessarily exactly that number each time. Clearly, if $m > 1$, then Eve will have a good chance of being able to split the pulses, observing one photon while letting the remainder continue undisturbed to Bob. If m is significantly less than 1, then the probability of an eavesdropper being able to split the pulse is approximately $m^2/2$ [27]. Even in this case the eavesdropper will be able to learn a constant fraction of the key bits without being detected.

Up to now, an overview of one the most important protocols in QKD, the BB84, has been given. Although the security of QKD relies on the laws of quantum mechanics, it can be seen how a considerable part of the protocol takes place using exclusively the classical communication channel. Once the raw key has been transmitted over the quantum channel, a secret key is distill using classic post-processing techniques that require interaction, some information about the key is exchanged via the public channel in order to correct the errors and eliminate the possible information that Eve may have derived. Information Reconciliation is a mechanism that allows to eliminate the discrepancies between two correlated variables. It is an essential component in every key agreement protocol where the key has to be transmitted through a noisy channel. Hence, it is important to explore other classical techniques in the context of QKD systems, to minimize the information exchanged over the public channel so jeopardizing the provable security that quantum physics guarantees can be avoided.

Chapter 4

Low-Density Parity-Check codes

4.1 Noisy-channel Coding Theorem

In information theory, the noisy-channel coding theorem establishes that for any given degree of noise in a communication channel, it is possible to communicate discrete data (digital information) nearly error-free through the channel up to a computable maximum rate. This result was presented by Claude Shannon in 1948 [28] and was based in part on earlier work and ideas of Harry Nyquist and Ralph Hartley.

The Shannon limit or Shannon capacity of a communication channel is the theoretical maximum information transfer rate of the channel, for a particular noise level.

4.1.1 Overview

The theorem describes the maximum possible efficiency of error-correcting methods versus levels of noise, interference and data corruption. The notion of capacity is defined purely in terms of information theory. As such it does not guarantee the existence of transmission schemes that achieve the capacity.

The Shannon theorem states that given a noisy channel with channel capacity C and information transmitted at a rate R, then if $R < C$ there exist codes that allow the probability of error at the receiver to be made arbitrarily small. This means that, theoretically, it is possible to transmit information nearly without error at any rate below a limiting rate, C.

The converse is also important. If $R > C$, an arbitrarily small probability of error is not achievable. All codes will have a probability of error greater than a certain positive minimal level, and this level increases as the rate increases. So, information cannot be guaranteed to be transmitted reliably across a channel at rates beyond the channel capacity. The theorem does not address the rare situation in which rate and capacity are equal.

In the same paper Shannon introduced the concept of codes as ensembles of vectors that are to be transmitted. It is clear that if the channel is such that even one input element can be received in at least two possible ways, then reliable communication over that channel is not possible if only single elements are sent over the channel. This is the case even if multiple elements are sent that are not correlated.

To achieve reliable communication, it is thus imperative to send input elements that are correlated. This leads to the concept of a code, defined as a (finite) set of vectors over the input alphabet. We assume that all the vectors have the same length, and we denote this length as the block length of the code. If the number of vectors is $K = 2^k$, then every vector can be described with k bits.

Suppose now that a codeword is sent, and a vector is received over the output alphabet. If the channel allows for errors, then there is no general way of telling which codeword was sent with absolute certainty. However, it is possible to find the most likely codeword that was sent, in the sense that the probability that this codeword was sent given the observed vector is maximized. To find such a codeword, it is necessary to list all the K codewords, and calculate the conditional probability for the individual codewords. Then find the vector or vectors that yield the maximum probability and return one of them. This decoder is called the maximum likelihood decoder. It is not perfect: it takes a lot of time (especially when the code is large) and it may generate error, but it is the best that can be done.

Shannon proved the existence of codes of rates arbitrarily close to capacity for which the probability of error of the maximum likelihood decoder goes to zero as the block length of the code goes to infinity[1].

Achieving capacity is only part of the story. If these codes are to be used for communication, fast algorithms for encoding and decoding are needed. Note that random codes of rate R are just $2^{R \cdot n} = 2^{(k/n)n}$ random vectors of length n over the input alphabet. Some description of these vectors is needed in order to embed information into them, or it will be necessary to write all of them down into a so-called *codebook* describing which sequence of $R \cdot n$ bits gets mapped into which codeword. This will require a codebook of size $2^{R \cdot n}$, which is too large for any reasonably sized code[2]

If the input alphabet has the structure of a field (for example the binary alphabet which yields the field $\mathbb{F}_2$), then the complexity of the algorithm, as far as encoding goes, can be reduced. Golay [29] and Elias [30] independently introduced the concept of linear codes of block length n and dimension k defined as subspaces of the vector space ${\mathbb{F}_2}^n$. Such codes have rate k/n, and since they are linear, they can be described in terms of a basis consisting of k vectors of length n. A codebook

[1] In fact, Shannon proved that the decoding error of the maximum likelihood decoder goes to zero exponentially fast with the block length.

[2] For example consider a vector length of 1000 and code rate of 0.5, this yields 2^500 vectors, a codebook too large to handle).

can now be implicitly described by mapping a bit vector (x_1,x_2,...,x_k) to the vector obtained by taking linear combinations of the basis vectors given by the coefficients x_1,x_2,...,x_k. The class of linear codes is very rich. Shannon's arguments can be used to show that there are sequences of linear codes with rates arbitrarily close to capacity and for which the error probability of the maximum likelihood decoder approaches zero(exponentially fast) as the block length goes to infinity. Moreover, it can also be shown that random linear codes achieve capacity. Unlike their non-linear brothers, linear codes can be encoded in polynomial time, rather than exponential time. However, the decoding problem still remains. since the maximum likelihood problem on the binary symmetric channel (BSC) has been shown to be NP-hard[3], it is unlikely to find polynomial time algorithms for maximum likelihood decoding of general linear codes [31], for many classes of linear codes (e.g., general linear codes over $\mathbb{F}_q$ for any q).

4.2 Channel Capacity Definition

Consider the following block diagram representing a communication system:

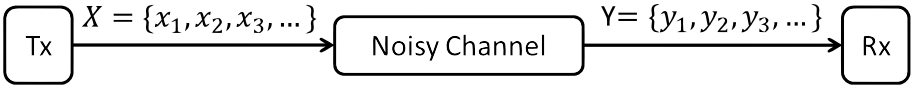


Figure 4.1: Simplified Block diagram: Transmission over a noisy channel

Let X represent the space of signals that can be transmitted, and Y the space of signals received, during a block of time over the channel. Let $p_{Y|X}(y|x)$ be the conditional distribution function of Y given X. Treating the channel as a known statistic system, $p_{Y|X}(y|x)$ is an inherent fixed property of the communications channel (representing the nature of the noise in it). Then the joint distribution $p_{X,Y}(x,y)$ of X and Y is completely determined by the channel and by the choice of the marginal distribution of signals chosen to be sent over the channel $p_X(x)$

$$p_X(x) = \int_y p_{X,Y}(x,y)dy$$

The joint distribution can be recovered by using the identity:

$$p_{X,Y}(x,y) = p_{Y|X}(y|x)p_X(x)$$

[3]The class NP is defined to be the set of computational problems which can be solved by a backtrack-search algorithm, where the depth of search is bounded by a polynomial in the length of the input. Alternately, NP is the set of problems solvable by a nondeterministic algorithm whose running time is bounded by a polynomial in the length of the input. A nondeterministic algorithm is one which, when confronted with a choice between two alternatives, can create two copies of itself and simultaneously follow the consequences of both courses. This repeated splitting may lead to an exponentially growing number of copies; the algorithm is said to solve the given problem if any one of these copies produces the correct answer. This description explains the notation: NP corresponds to the class of nondeterministic polynomial-time algorithms.

Under these constraints, the mutual information is defined as follows:

$$I(X,Y) = \int_Y \int_X p_{X,Y}(x,y) log \left(\frac{p_{X,Y}(x,y)}{p_X(x) p_Y(y)} \right)$$

Finally, the information channel capacity is defined as the maximum mutual information:

$$C = \max_{p(x)} I(X,Y) \tag{4.1}$$

where the maximum is taken over all possible input distributions $p(x)$.

4.2.1 Binary Symmetric Channel

A binary symmetric channel BSC_p is a kind of communication channel with binary inputs and outputs respectively. A probability p is associated with BSC_p is called the *cross-over probability*. This means, with a probability P, a bit sent through the BSC_p is flipped. And conversely with a probability $1 - p$ a bit sent through the BSC_p passes unchanged. In the case of the BSC_p, the capacity of the channel can be calculated as follows. By definition, the classical capacity is the maximum of the mutual information taken over all possible input distributions:

$$I(X,Y) = H(Y) - H(Y|X) = H(X) - H(X|Y)$$

Is known that the mutual information is defined as:

$$I(X,Y) = H(Y) - H(Y|X) = H(X) - H(X|Y)$$

Where the conditional entropy can be calculated using the following expression:

$$H(X|Y) = H(X|Y = 0)P(Y = 0) + H(X|Y = 1)P(Y = 1)$$

The conditional entropy per bit can be defined as:

$$H_b(p) = H(X|Y = 0) = H(X|Y = 1) = p \ log \ \left(\frac{1}{p} \right) + (1 - p) \ log \ \left(\frac{1}{1 - p} \right)$$

So the mutual information can be rewritten as follows:

$$H(X|Y) = H_b(p) \rightarrow I(X,Y) = H(X) - H_b(p)$$

Since $H(X)$ is known

$$H(X) = P_0 \ log \ \left(\frac{1}{P_0} \right) + (1 - P_0) \ log \ \left(\frac{1}{1 - P_0} \right) = H_b(p_0)$$

Finally, the expression for the mutual information of the BSC_p is:

$$I(X,Y) = H_b(P_0) - H_b(P_e)$$

Where $H_b(P_0) = P_0 log\,(1/P_0) + (1 - P_0) log\,(1/1 - P_0) \leq 1$

Notice that, when the binary input symbols are equiprobable, i.e. $P_0 = P_1 = 0.5$, H_b reaches its maximum value $H_b = 1$, maximizing the mutual information, so the channel capacity is equal to $C = 1 - H_b(p)$. In Figure 4.2, the capacity C of the BSC_p is shown, as a function of the cross-over probability, i.e. error probability, P. It can be seen that C=0 when P=1/2 and C=1 when P=0 or P=1

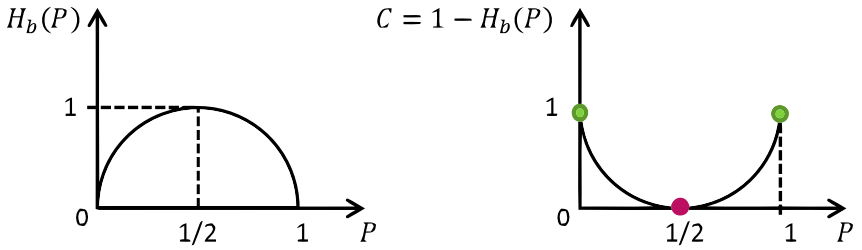


Figure 4.2: Capacity of a BSC for a two equiprobable input symbols and a crossover probability P

4.3 Linear Block codes

It is assume that the output of an information source is a sequence of binary digits "0" or "1". In block coding, this binary information sequence is segmented into message blocks of fixed length. Block codes refers to the large and important family of error-correcting codes that encode data in blocks. Error correction is obtained by adding redundant symbols to a codeword.

If k symbols are sent into the coder, n symbols are obtained as an output of it. The rate of a code is:

$$R = k/n$$

It is always the case for error correction that $R < 1$.

A desirable property for a linear block code to possess is the systematic structure of the codewords, where a codeword is divided into two parts, the message part and the redundant checking part. The message part consists of k unaltered information (or message) digits and the redundant checking part consists of n-k parity-check digits, which are linear sums of the information digits. A linear block code with this structure is referred to as a linear systematic block code.

Let the message $\bar{m} = (m_0,m_1,...,m_{k-1})$ be an arbitrary k-tuple from GF(2). The linear (n, k) code over $GF(2)$ is the set of 2_k codeword of row-vector form $\bar{c} = (c_0,c_1,...,c_{k-1})$

where $c \in GF(2)$. By linear transformation:

$$\bar{c} = \bar{m} \cdot \mathbf{G} = \sum_{i=0}^{k-1} \bar{m}_i \cdot \bar{g}_i = m_0 g_0 + m_1 g_1 + ... + m_{k-1} g_{k-1}$$

Where $\mathbf{G}$ is a $k \times n$ matrix of rank k of elements from GF(2), $\bar{g}_i$ is the *i-th* row vector of $\mathbf{G}$.
$\mathbf{G}$ is called the *generator matrix* of the code. The rows of $\mathbf{G}$ are linearly independent since $\mathbf{G}$ is assumed to have rank k.

An (n,k) block code is said to be linear if the vector sum of two codewords is a codeword.

For each linear code there is also a *parity check matrix* $\mathbf{H}$ with the following property: An n-tuple $\bar{c}$ is a codeword if and only if it is orthogonal to every row vector of $\mathbf{H}$:

$$\bar{c} \cdot \mathbf{H}^T = 0 \Leftrightarrow \bar{c} \text{ is a codeword.}$$

And since the rows of $\mathbf{G}$ are possible codewords. then:

$$\mathbf{G} \cdot \mathbf{H}^T = 0$$

For any given generator matrix $\mathbf{G}$, many solution for $\mathbf{H}$ are possible.

4.4 LDPC codes

Low-density parity-check (LDPC) codes are a class of linear block LDPC codes. The name comes from the characteristic of their parity-check matrix which contains only a few 1's in comparison to the amount of 0's. Their main advantage is that they provide a performance which is very close to the capacity for a lot of different channels and linear time complex algorithms for decoding. Furthermore are they suited for implementations that make heavy use of parallelism.

They were first introduced by Gallager in his Ph.D. thesis in 1960 [32]. But due to the computational effort in implementing coder and encoder for such codes and the introduction of Reed-Solomon codes [33], they were mostly ignored until about ten years ago.

A family of LDPC codes is usually defined by two generating polynomials:

$$\lambda(x) = \sum_{i=2}^{d_{v_{max}}} \lambda_i x^{i-1}$$

$$\rho(x) = \sum_{i=2}^{d_{c_{max}}} \rho_i x^{i-1}$$

The coefficients of these polynomials define the distribution of incident edges to variable and check nodes respectively. Richardson et al. showed that the asymptotic behavior of a family of codes defined by both polynomials can be analyzed by using the density evolution algorithm [34]. Families of LDPC codes performing close to the channel capacity can be then designed by optimizing both generating polynomials [35],[36].

An LDPC code is a linear code identified by an sparse parity-check matrix or its equivalent bipartite graph, also called Tanner graph. It is known that some iterative algorithms, such as belief propagation based algorithms, provide optimum decoding over cycle-free Tanner graphs [37]. However, any finite-length graph has necessarily cycles, and it has been shown that a large girth (length of the shortest cycle) improves the performance of LDPC codes using iterative decoding as it enforces a reasonable minimum distance[38]. Therefore, taking into account that a finite-length graph has cycles, it is important to make its girth as large as possible.

4.4.1 Representations for LDPC codes

Basically there are two different possibilities to represent LDPC codes. Like all linear block codes they can be described via matrices. The second possibility is a graphical representation.

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

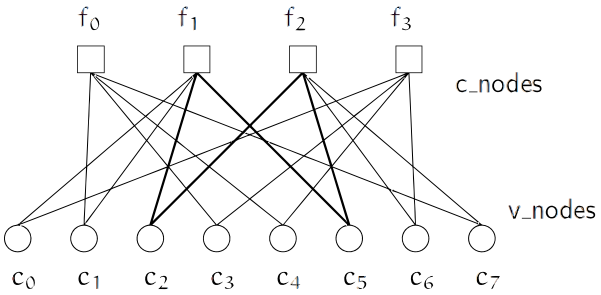


Figure 4.3: Tanner graph corresponding to the parity check matrix $\boldsymbol{H}$. The marked path $c2 \rightarrow f1 \rightarrow c5 \rightarrow f2 \rightarrow c2$ is an example for a short cycle. Those should usually be avoided since they are bad for decoding performance.

Matrix Representation

Let $\mathbf{H}$ be a binary $n \times m$-matrix, then the LDPC code defined by the matrix $\mathbf{H}$ is the set of vectors $c = (c_1,c_2,...,c_m)$ such that $H \cdot c^T = 0$. The matrix H is called a

parity check matrix for the code. The matrix shown in figure 4.3 is a parity check matrix with dimension $n \times m$ for a (8,4) code. We can now define two numbers describing these matrix. w_r for the number of 1's in each row and w_c for the number of 1's in the columns. For a matrix to be called low-density the two conditions $w_c \ll n$ and $w_r \ll m$ must be satisfied. In order to do this, the parity check matrix should usually be very large, so the example matrix cant be really called low-density.

Graphical Representation

Tanner introduced an effective graphical representation for LDPC Tanner codes [37]. Not only provide these graphs a complete representation of the graph, they also help to describe the decoding algorithm. Tanner graphs are bipartite graphs. The nodes of the graph are separated into two distinctive sets and edges are only connecting nodes of two different types. The two types of nodes in a Tanner graph are called variable nodes (v-nodes) and check nodes (c-nodes).

Figure 4.3 is an example for such a Tanner graph and represents the same code as the matrix **H**. The creation of such a graph is rather straight forward. It consists of m check nodes (the number of parity bits) and n variable nodes (the number of bits in a codeword). Check node f_i is connected to variable node c_j if the element h_{ij} of H is a 1.

4.4.2 Decoding Algorithms: Belief Propagation

A general class of decoding algorithms for LDPC codes is denoted as *message passing* algorithms. These are iterative algorithms in which at each round messages are passed from variable nodes to check nodes, and from check nodes back to variable nodes. The messages from variable nodes to check nodes are computed based on the observed value of the variable node and some of the messages passed from the neighboring check nodes to that variable node. An important aspect is that the message that is sent from a variable node v to a check node c must not take into account the message sent in the previous round from c to v. The same is true for messages passed from check nodes to message nodes.

One important subclass of message passing algorithms is the belief propagation algorithm. This algorithm is present in Gallager's work [32]. The messages passed along the edges in this algorithm are probabilities, or beliefs. More precisely, the message passed from a variable node v to a check node c is the probability that v has a certain value given the observed value of that message node, and all the values communicated to v in the prior round from check nodes incident to v other than c. On the other hand, the message passed from c to v is the probability that v has a certain value given all the messages passed to c in the previous round from message nodes other than v.

One very important aspect of belief propagation is its running time. Since the algorithm traverses the edges in the graph, and the graph is sparse, the number of edges traversed is small. Moreover, if the algorithm runs for a constant number of times, then each edge is traversed a constant number of times, and the algorithm uses a number of operations that is linear in the number of message nodes.

Another important note about belief propagation is that the algorithm itself is entirely independent of the channel used, in spite of the fact that the messages passed during the algorithm are completely dependent on the channel.

4.4.3 LDPC Convergence Analysis

A typical decoded bit error performance curve of an iteratively decoded capacity achieving code transmitted over a binary symmetric channel (BSC), as a function of the transition probability P of the BSC, is illustrated in 4.4

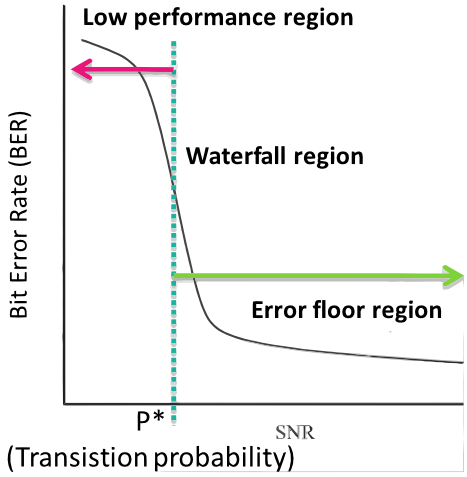


Figure 4.4: Typical decoded BER performance curve of an iteratively decoded capacity achieving code

The performance of the code is divided into three regions: the low-performance region, the waterfall region and the (optional) error floor region.

The low-performance region is the region where the transition probability P is higher than the minimum value required for the iterative decoding to converge. The value of the threshold transition probability P* depends on the length of the considered code.

The performance region where a small decrease in the transition probability P results in a considerable improvement in the error probability is called the *waterfall region* or, sometimes, the *turbo cliff region*, when its slope is particularly steep.

In the error floor region, when present, the performance does not improve significantly as the transition probability P decreases further, or however it decreases with a slope much smaller than in the waterfall region. We must note that the error floor region typically does not show a horizontal floor, but a change in slope with respect to the waterfall region.

Given these general characteristics of an LDPC code performance, and knowing that a quantum channel has a typical quantum bit error rate (or quantum BER or QBER) $Q \leq 0.11$, and that the channel is not considered reliable because of eavesdropping if $Q > Q* \approx 0.15$[4], the non-convergence could be detected by observing the erratic behavior of the decoded sequence reliability, allowing the use of the decoded codeword reliability monitoring as a form of quantum channel probe. Hence, we can devise a novel mechanism of detecting eavesdropping on the fly based on the inherent characteristics of the codes employed for information reconciliation.

4.4.4 LDPC EXIT Charts

AnEXtrinsic Information Transfer chart, commonly called EXIT chart, is a technique to aid the construction of good iteratively-decoded error-correcting codes (in particularLDPC and Turbo codes).
An EXIT chart includes the response of the elements of decoder. The response can either be seen as extrinsic information or a representation of the messages inbelief propagation.
The belief propagation decoding explained in the previous section can be summarize as follows: Message Passing Algorithm (Belief Propagation)

1. Initialize variable nodes with observations from channel
2. Variable-node decoding: Take all incoming messages and compute messages to check nodes
3. Check-node decoding: Take all incoming messages and compute messages to variable nodes
4. Repeat 2 and 4 until a termination criterion is fulfilled

In Figure 4.5 a simplified block diagram of an LDPC iterative decoding is shown, with the intention to illustrate the construction of LDPC EXIT charts. The following hypotheses are taken into account:

[4] i.e., if the QBER is larger than a given threshold Q*, if an LDPC code is selected with threshold transition probability $P* \approx Q*$, the decoding process will not converge if the quantum channel is unreliable

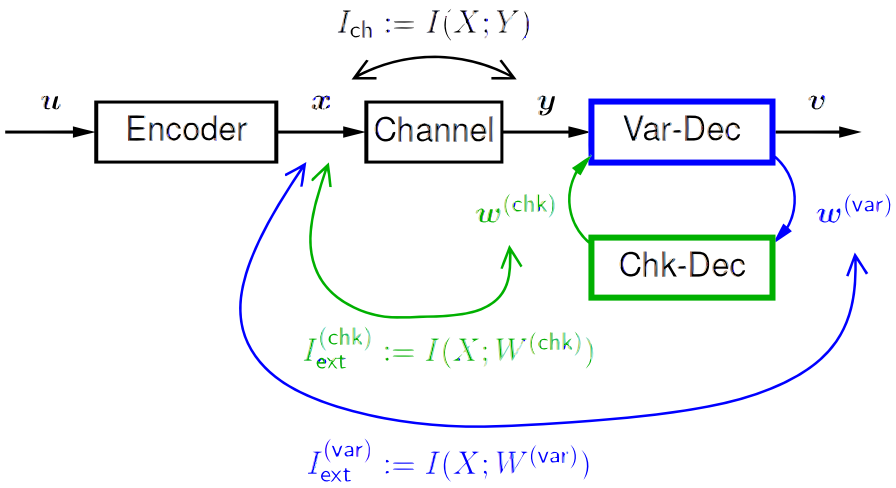
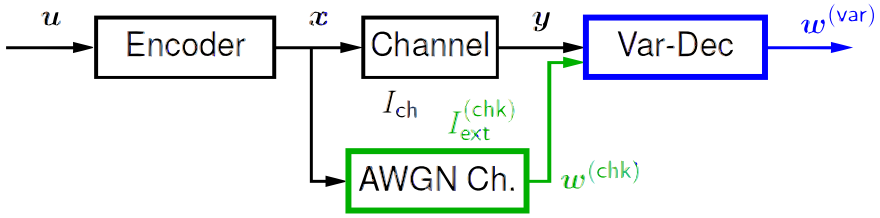
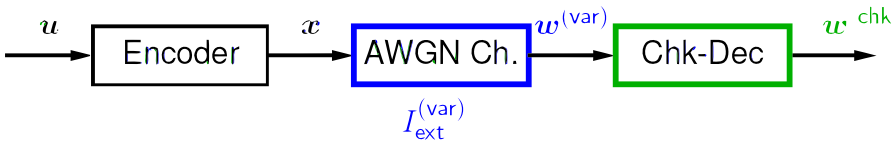


Figure 4.5: Block Diagram for the construction of LDPC EXIT Charts

- Virtual channel $X \rightarrow W^{(chk)}$ is modeled by an AWGN channel with mutual information $I_{ext}^{(chk)}$. The simluation of the variable-node decoder gives the variable-node EXIT function.

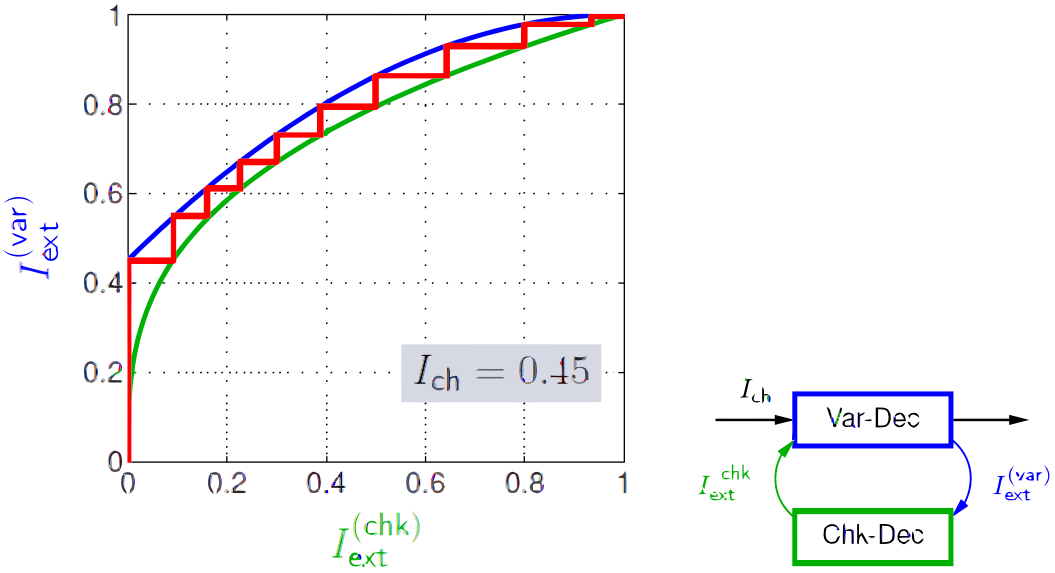


- Virtual channel $X \rightarrow W^{(var)}$ is modeled by an AWGN channel with mutual information $I_{ext}^{(var)}$. The simluation of the check-node decoder gives the check-node EXIT function.



The EXIT Chart shows the information transfer for LDPC decoding and the performance of LDPC decoding in the fall-off region. It plots the mutual information of the variable nodes decoder one versus the mutual information of the check nodes decoder which is modeled by the test (a priori) channel. In other words the output

of the left branch in Figure 7.9 determines the value of the horizontal axis of the EXIT chart and the output of the right branch determines the value on the vertical axis. Both range between 0 and 1. For the next (half) iteration both decoders are swapped and interchange their roles: the output of decoder one becomes the a priori input of decoder number two. Only the extrinsic values are used as output, meaning that the a priori input value is subtracted from the full soft output. This avoids propagation of already known information.



(a) EXIT Chart

(b) Iterative Decoder

Figure 4.6: LDPC EXIT Chart

Chapter 5

Soft-metric QKD Protocol

In chapter 3 an overview of current QKD systems (based on interactive error correction and information reconciliation protocols) has been given. The fact that an important part of the protocol takes place using exclusively classical communication schemes has been remarked, specially because BB84-like schemes are based on a highly interactive process that requires many communication rounds. BB84-like protocols for error correction and information reconciliation in QKD systems are not very efficient in terms of throughput (distilled key per second) since a lot of information is discarded to ensure that the information Eve can possibly know is canceled from the final secret key.

It is in this scenario that modern Forward Error Correction (FEC) schemes may offer an interesting solution. The idea is to make use of FEC's inherent advantage of requiring a single channel use to reconcile the set of transmitted and received bits (qubits in the case of QKD). In order to maximize the system performance, capacity achieving codes are preferable, and LDPC codes constitute a possible interesting option.

In this chapter, in particular, we have focused our attention on the use of LDPC codes decoded with a message-passing decoding algorithm [39] for information reconciliation in QKD applications. A "composite communication channel" composed of the parallel of the quantum channel and the public channel of a QKD scheme is considered. LDPC codes are suggested -in the context of QKD schemes- to perform error reconciliation through feed-forward error correction, minimizing the interaction between transmitter and receiver. A protocol focused on pragmatic information reconciliation applied to QKD schemes using soft information processing techniques is proposed.

5.1 Information Reconciliation

Let X and Y be two of correlated variables belonging to Alice and Bob, and x and y their outcome strings, through information reconciliation it is possible to

eliminate the discrepancies between x and y and agree on a string $S(x)$, with possibly $S(x) = x$.

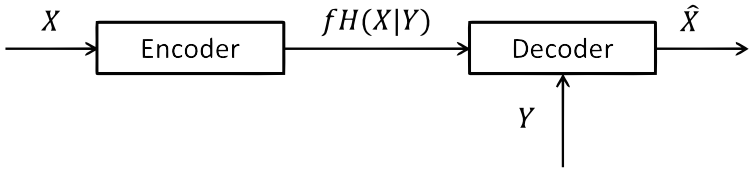


Figure 5.1: Source coding with side information

The problem of information reconciliation in QKD schemes can be seen as the source coding problem with side information, as shown in Figure 5.1. Thus, as shown by Slepian and Wolf [40], the minimum information I that Alice would have to send to Bob in order to help him reconcile Y and X is $I_{opt} = H(X|Y)$. Taking into account that real reconciliation will not be optimal, a parameter $f > 1$ is used as a quality figure for the reconciliation efficiency:

$$I_{real} = f \cdot H(X|Y) > I_{opt}$$

5.2 QKD Protocol Generalities

For the generic model of any QKD scheme, Alice wants to transmit a plaintext message secretly to the receiver Bob. The secret key is transmitted on a secure (quantum) channel, which has typically high bit error rate, that will denoted as $QBER$, so that a subsequent information reconciliation and privacy amplification operations need to be performed on a public channel. Once the secret key is known to Alice and to Bob (and only to them), Alice will encrypt the plaintext using the secret key according to the encryption rule of the system, and send the cryptogram to Bob, while Eve will not be able to recover the transmitted message.

The protocol proposed in this thesis, considers the problem of information reconciliation as if it were the source coding problem with side information. It is focused on effective forward error correction which exploits the "soft-information" available at the exit of both the quantum and the public channel.

In figure 5.2 a very simplified scheme of a generic QKD platform is presented. A *composite channel* can be identified, formed by the parallel of the quantum and the public channels. The information and redundancy bits transmitted by these two communication systems constitute the codewords of an equivalent systematic block code. Alice divides the original information bit stream into *blocks* of finite length n_q which will be encoded in a redundant way into *codewords* of length n.

The information bits (n_q bits per codeword) are transmitted over the quantum *private* channel, while the redundancy bits ($r = (n-n_q)$ bits per codeword) are transmitted over the classical *public* channel. The code rate (or information rate) is equal

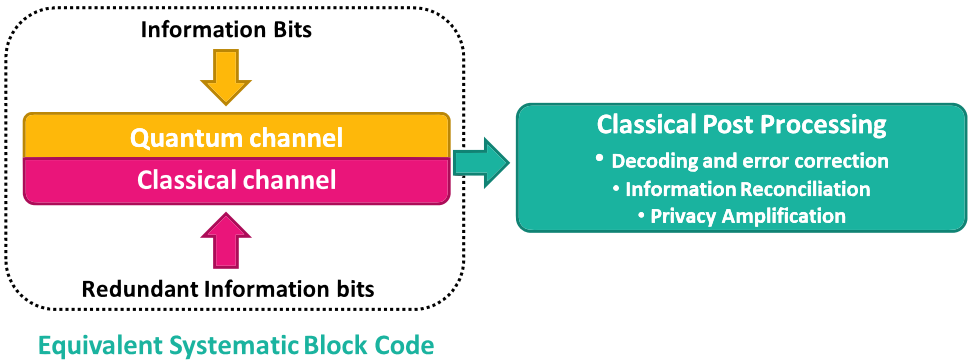


Figure 5.2: Equivalent systematic block-code in QKD system

to k/n which is the proportion of the data-stream that is useful (non-redundant)[1]. The redundancy allows the receiver to detect and correct errors without retransmission, using *Forward Error Correction* techniques. In this context, iterative belief propagation algorithms can be used to decode the *codewords* sent by Alice at the receiving stage, with a maximum likelihood decoding rule.

As previously mentioned, LDPC codes with possibly long information blocks have been selected to make the quantum channel more reliable. This choice is motivated by the characteristics of LDPC codes of being asymptotically capacity achieving and of being decodable in a time linearly proportional to their block length (when iterative belief propagation techniques are used), so that acceptable decoding complexities can be achieved also for large block lengths.

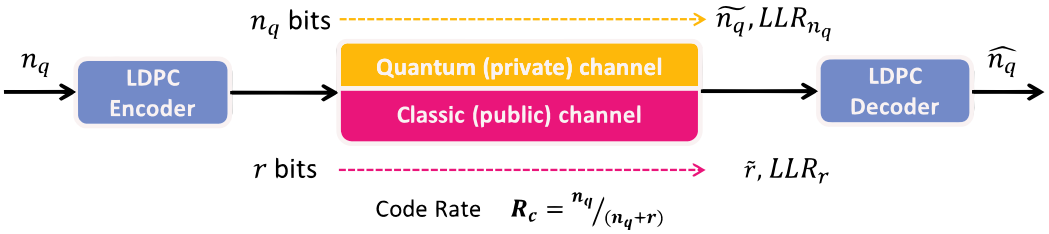


Figure 5.3: Composite Channel model, LDPC with code rate $n_q/(n_q + r)$

To minimize the quantity of information derived by Eve from the public channel the code rate must be maximized. In figure 5.3 the rate code along with the number of available information and redundancy bits are highlighted, for a code with a rate equal to $n_q/(n_q+r) = n_q/n$. It is important to notice that at the input of the LDPC decoder, there will be n total available bits, i.e. n corresponding loglikelihood values.

[1]That is, if for every n_q bits of useful information, the coder generates totally n bits of data, of which r are redundant

In a generic QKD system, such as the one shown in figure 5.4, many attacks strategies could hypothetically be used by Eve. The eavesdropping on the secure channel is shown as a dotted line, because - if the system is properly designed - the presence of Eve can be detected, and the information leaked to Eve can be made arbitrarily small, as if the eavesdropper did not exist. Given this hypothesis, the next sections will focus on the overall channel model linking Alice to Bob, neglecting for now the effect of Eve.

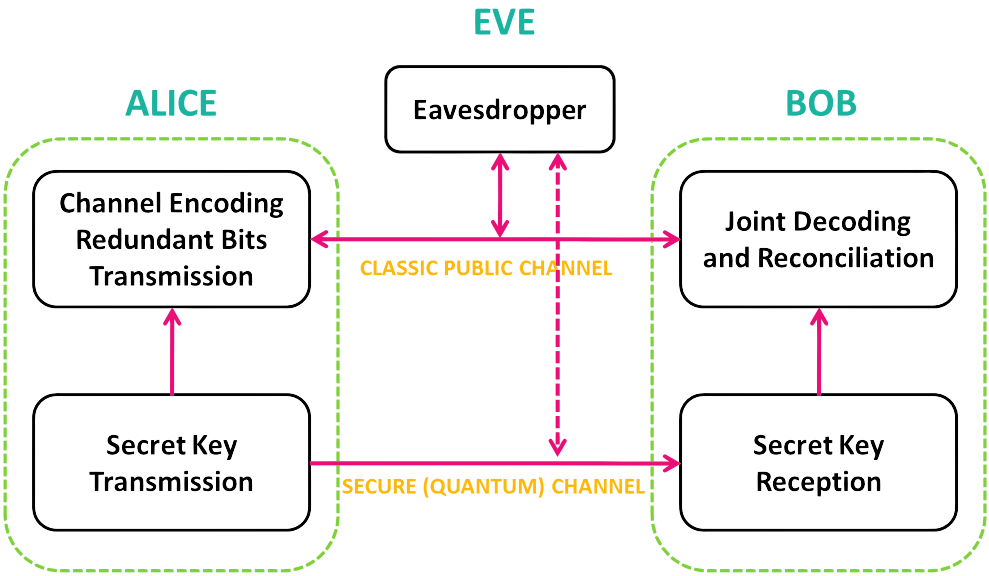


Figure 5.4: Quantum Key Distribution Protocol

The transmission rate on the QKD secret channel is generally very low since the technology is very complex, while the actual data rate on the public channel can be very high. It is therefore important to analyze the achievable overall QKD system rate. Furthermore, in practical cases, the quantum bit error rate on the secret channel is typically high when compared to the bit error rate of the public channel.

5.2.1 FEC Coding Rate and its Impact on Security

The information transmitted on the classic public channel is completely visible to the eavesdropper Eve. In the security analysis it must be assumed that Eve has perfect knowledge of the code, and therefore of the r parity check equations used to generate the r parity bits ($(n\text{-}n_q)$ redundancy bits), that are assume to be received (eavesdropped) perfectly and without errors. The question then is how much information can Eve obtain about the n_q information/data bits from the knowledge of the r parity bits.

The r parity check equations represent a system of r linear equations in n_q variables over GF(2). This system in the case of LDPC codes is indeed quite sparse (i.e., few variables appear in each check equation). The space of solutions of such a system of equations represents the set of possible data sequences that Eve has access to. One of these solutions is in fact, the true data transmitted through the private quantum channel. The larger the size of the space of possible sequences, the more secure is the FEC code used against Eve. This assumes that Eve does not possess any additional information that may reduce the space of possible sequences. For instance, if the data transmitted by Alice is not independent identically distributed (i.i.d.) (i.e. binary with equal probabilities), Eve can easily focus on the most probable set of possible solutions of the linear equations. Note that the structural properties of the particular LDPC code used, ultimately determines the extent of the security of the system.

Let the data sequence transmitted over the private quantum channel be denoted by the n_q-component vector $\vec{X}$, and the parity checks transmitted over the classic public channel by the r-component vector $\vec{P}$.

The amount of information provided about $\vec{X}$ by $\vec{P}$ is the mutual information $I(\vec{X},\vec{P}) = H(\vec{P}) - H(\vec{P}|\vec{X}) = H(P) \leq r$, since $H(\vec{P}|\vec{X}) = 0$ (i.e., given $\vec{X}$, the amount of uncertainty remaining about $\vec{P}$ is zero).

Remembering that the quantum channel operates in conjunction with a classic public channel, together with the information bits the redundancy (parity check) bits generate an equivalent block code with rate:

$$R_c = \frac{n_q}{n_q + r} \tag{5.1}$$

So long as $n_q > 0$, a secret key can be distilled for a fixed code rate by increasing the block length. This puts a lower limit on the coding rate $\frac{1}{1+r/n_q}$ of 0.5, which nonetheless is loose since the security of the scheme even at coding rate 0.5 or below ultimately depends on the particular FEC code being used.

5.3 Classical Communication System

The public channel uses classic communication schemes, and possibly strong coding, so that the bit error rate of the classic channel is generally extremely low. Since the use of an optical link implies the presence of line of sight (LOS) between transmitter and receiver, fading can be excluded, and additive white Gaussian noise (AWGN) is generally the predominant impairment. Thus, the equivalent channel model shown in Figure 5.5 can be considered to represent a classic "public" channel in the QKD protocol being proposed.

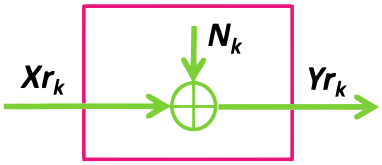


Figure 5.5: Classical Communication Channel

In this model, when a bipolar transmission scheme is used such as PAM, BPSK or Gray coded QPSK, the k-th transmitted redundant bit is $b_k \in (0,1)$, the associated k-th transmitted symbol is $X_{r_k} \in (-\sqrt{E_b}, +\sqrt{E_b})$, i.e. $X_{r_k} = \sqrt{E_b}(2b_k - 1)$, while $N_k \in \mathrm{N}(0,\sigma^2)$ is a Gaussian random variable with zero mean and variance equals to $\sigma^2 = N_0/2 = E_b/2\eta_S$, where $\eta_S = E_b/N_0$ is the wireless link signal-to-noise ratio, and Yr_k is the received sample obtained at the output of the public channel detector.

Figure 5.6: Representation of the classic "public" channel

Despite the fact that for simulations purposes a bipolar transmission scheme (PAM or BPSK) has been considered, the extension for different modulation schemes is straightforward.

On the public link, no information bits can be transmitted, so only the redundant information of the considered feed-forward systematic block channel code with rate R will be transmitted. The expression for the Log-Likelihood metrics at the output of the classical channel is given by the following expression:

$$LLR(Y_{r_k}) = log\left[\frac{p(X_{r_k} = +\sqrt{E_b}|Y_{r_k})}{p(X_{r_k} = -\sqrt{E_b}|Y_{r_k})}\right] = log\left[\frac{p(Y_{r_k}|X_{r_k} = +\sqrt{E_b})}{p(Y_{r_k}|X_{r_k} = -\sqrt{E_b})}\right] = log\left[\frac{p(Y_{r_k}|b_k = 1)}{p(Y_{r_k}|b_k = 0)}\right] \tag{5.2}$$

Equation 5.2 has been rewritten using Bayes' Theorem[2].

Given the previous hypotheses, the expressions for the k-th trasmitted and received symbols respectively, can be written as:

$$X_{r_k} = \sqrt{E_b}(2b_k - 1) \tag{5.3}$$

$$Y_{r_k} = X_{r_k} + N_k = \sqrt{E_b}(2b_k - 1) + N_k \tag{5.4}$$

[2]Bayes' Theorem: $P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}$

Y_{r_k} are the real signal samples being received, whose conditional probability density function is given by the Equation 5.5

$$f_y(Y_{r_k}|b_k) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{-(Y_{r_k}-\sqrt{E_b}(2b_k-1))^2}{2\sigma^2}} \tag{5.5}$$

Finally, replacing the expressions presented in Equations 5.3 into Equation 5.5 written above, the value of the LLR's metrics for the symbols received from the public channel can be expressed as:

$$LLR(Y_{r_k}) = log\left[\frac{p(Y_{r_k}|b_k=1)}{p(Y_{r_k}|b_k=0)}\right] = \frac{2Y_{r_k}\sqrt{E_b}}{\sigma^2} \tag{5.6}$$

This is the soft metric associated to the k-th redundant bit, associated to the sample Y_{r_k} at the output of the classic channel.

5.4 Quantum Communication System

In this section, the problem of how to describe the quantum channel is considered and discussed, with the aim to find an analog in the classical world and to determine its capacity.

The usual starting point for information theory is to model the communication channel stochastically. A channel is usually modeled as a noisy mapping of some input assemble x to an output assemble y according to some transition probabilities, $p(y|x)$. Then, channel's capacity can be found as a function of these parameters: it is defined as the maximum mutual information that can be generated between input and output given a single use of the channel[3]. Some assumptions about the quantum channel are necessary to be able to model it using classical known schemes (see Appendix D).

Many practical scenarios can be consider when modeling a quantum channel: the transmitted qubit can be associated to a single photon or a multi-photon, and different specific quantum states can be transmitted over the quantum channel (coherent state, entangled state, squeezed state, etc).

In this thesis, both single photon and multi-photon transmission will be considered when characterizing the quantum communication system in the context of the proposed QKD protocol. When referring to multi-photon transmission, coherent states will be considered, generated using weak laser pulses (WLP) sources.

[3]Since there are several quantum mechanical effects that can affect the quantum transmission over the secure channel, the estimation of the quantum bit error rate has been done both through empirical research, produced by observations and experiments made at the INRiM (Istituto Nazionale di Ricerca Metrologica) by the research team of Prof. Genovese, and through theoretical calculation as well.

5.4.1 Single-Photon Quantum Channel

When a single-photon is transmitted, the quantum channel can be modeled as a simple binary channel with error probability equal to the quantum bit error rate (QBER) Q, as shown in Figure 5.7. This is a very general model that can be used, for example, to model the quantum channel when polarization encoding is applied to photons in protocols such as the BB84 or the B92 presented earlier in Chapter 3.

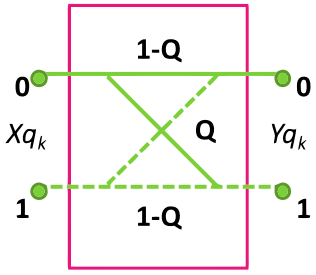


Figure 5.7: Quantum channel modeled as a Binary Symmetric Channel (BSC)

The expression for the Log-Likelihood metrics at the output of the quantum channel represented by the model of Figure 5.7 used as input for the soft-metric decoder, is given by:

$$LLR(Y_{q_k}) = log\left[\frac{p(X_{q_k}=1|Y_{q_k})}{p(X_{q_k}=0|Y_{q_k})}\right] = log\left[\frac{p(Y_{q_k}|X_{q_k}=1)}{p(Y_{q_k}|X_{q_k}=0)}\right] \tag{5.7}$$

Denoting the k-th transmitted information bit as $X_{q_k} \in GF(2) = \{0,1\}$, and the received information bit as $Y_{q_k} \in GF(2) = \{0,1\}$ Equation 5.7 can be rewritten as follows:

$$LLR(Y_{q_k}) = log\left[\frac{p(Y_{q_k}=1|X_{q_k})}{p(Y_{q_k}=0|X_{q_k})}\right] = \begin{cases} log\left(\frac{1-Q}{Q}\right) & \text{if } Y_{q_k}=1 \\ log\left(\frac{Q}{1-Q}\right) & \text{if } Y_{q_k}=0 \end{cases} \tag{5.8}$$

Notice that if the QBER value Q is not perfectly known, it should be substituted by its estimate Q_{est} [4].

It is also important to notice that the log-likelihoods (metrics) $LLR(Y_{q_k})$ can only assume two values, and will therefore be referred to as *hard metrics* or *q-metrics*, while the metrics from the public channel $LLR(Y_{r_k})$ can assume any real value, and are called *soft metrics*.

Since these metrics must be jointly used and compared in the LDPC decoder they need to be compatible and comparable. Suppose that the equivalent BSC model

[4] We denote as Q_{est} the estimated quantum channel bit error rate, which should ideally be equal to Q if the channel is completely known, or if it behaves as expected.

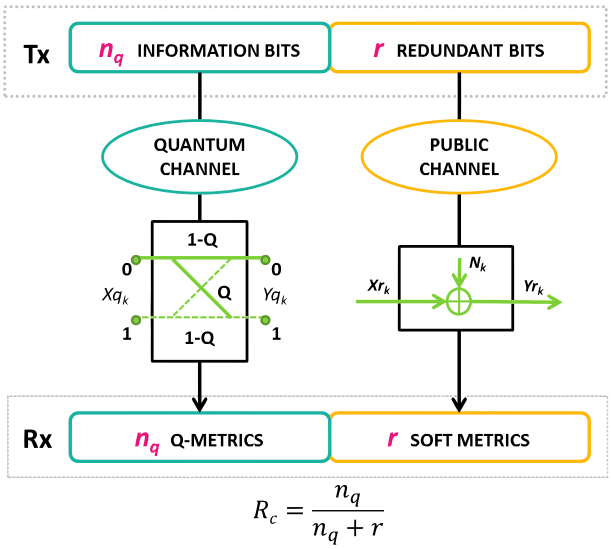


Figure 5.8: Available bits and metrics from the public and the quantum-BSC channels

used for the quantum channel is obtained using a 2PAM as modulation scheme with transmitted levels $\sqrt{E_{pb}}(2X_{q_k} - 1)$ where X_{q_k} are the transmitted bits, Y_{q_k} are the decided raw bits, E_{pb} is the energy per bit and σ_p^2 is the noise variance per dimension. Denoting the equivalent received sample as Y_{p_k}, we have $Y_{p_k} = \sqrt{E_{pb}}(2X_{q_k} - 1) + N_{p_k}$, and the theoretical quantum error probability equals:

$$p(X_{q_k} \text{ in error}) = \frac{1}{2} erfc \sqrt{\frac{E_{pb}}{2\sigma_p^2}} = Q \tag{5.9}$$

where, the transmitted levels are $\pm\sqrt{E_{pb}}$ and $N_{p_k} \in \mathcal{N}(0, \sigma_p^2)$ as shown in Figure 5.9.

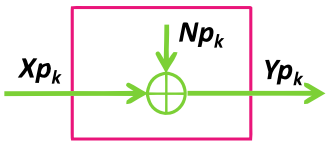


Figure 5.9: Equivalent model for the single-photon quantum channel when using an equivalent 2PAM modulation scheme.

Notice that we have as a consequence:

$$\frac{E_{pb}}{2\sigma_p^2} = erfc^{-1}(2Q)^2 \tag{5.10}$$

At this point assuming that the noise is negligible, (i.e., that $Y_{p_k} \cong \sqrt{E_{pb}}(2Y_{q_k} - 1) \cong \sqrt{E_{pb}}(2X_{q_k} - 1)$) allows to approximate the soft metric derived from the

quantum channel when using a 2PAM modulation as follows:

$$LLR(Y_{p_k}) = \frac{4Y_{p_k}\sqrt{E_{pb}}}{2\sigma_p^2} = \frac{4E_{pb}(2Y_{q_k}-1)}{2\sigma_p^2} \tag{5.11}$$

$$= 4[erfc^{-1}(2Q)]^2(2Y_{q_k}-1) = \begin{cases} +4[erfc^{-1}(2Q)]^2 & \text{if } Y_{q_k}=1 \\ -4[erfc^{-1}(2Q)]^2 & \text{if } Y_{q_k}=0 \end{cases} \tag{5.12}$$

Notice that the expression 5.11 constitutes an approximated metric for the equivalent BSC quantum channel of Figure 5.7, and can be used as an alternative to the actual metric shown in Equation 5.8, specially for analysis where the BSC quantum channel has to be modeled as an equivalent AWGN channel [41].

Binary Erasure Quantum Channel

In a time slotted system, if also the lost photons are taken into account, a channel model taking into account both errors and erasures can be considered. This model is similar to the binary erasure channel (BEC)[5], and it is shown in figure 5.10 for a quantum error probability q and an erasure probability e.

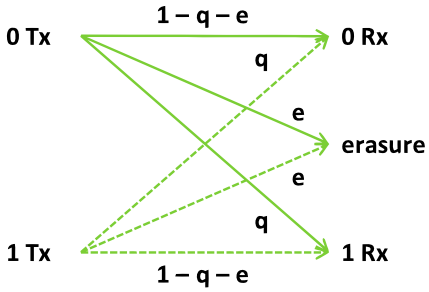


Figure 5.10: Binary Erasure Quantum Channel model

5.4.2 Multi-Photon Quantum Channel

As opposed to hard decisions about whether a given received signal is a logic-0 or a logic-1, the use of a Photon Counting Detector (PCD) is suggested to generate soft information at the output of the quantum channel. Consider the application of soft coding to a specific scheme, i.e., the one shown in Figure 5.4.

In reference to the model depicted in Figure 5.4, when transmitting multi-photons over the quantum channel, the practical implementations of QKD protocols rely on solutions that are low cost, offer high levels of security, and can be rapidly deployed

[5] A binary erasure channel (or BEC) is a common communications channel model used in coding theory and information theory, introduced by Peter Elias at MIT in 1954 as a toy example. In this model, the transmitter sends a bit, and the receiver either receives the bit or it receives the message that the bit was not received ("erased").

requiring uncomplicated setups and conventional devices. In this regard, the use of decoy states is currently the most promising technique.

Decoy states

Decoy state Quantum key distribution (DQKD) protocols have been proposed to solve the multi-photon issue in QKD sources. In QKD protocols, such as BB84, a single-photon source is assumed to be used by the sender, Alice. In reality, a perfect single-photon source does not exist. Instead, practical sources, such as weak coherent state laser sources, are widely used for QKD. The key problem with these practical QKD sources is the multi-photon components within. A serious security loophole exists when Alice uses multi-photon states as quantum information carriers[6]. In order to minimize the effects of multi-photon states, Alice has to use an extremely weak laser source, which results in a relatively low speed QKD. Decoy state QKD is proposed to solve this multi-photon issue by using a few different photon intensities instead of one. With decoy states, the practical sources, such as coherent-state sources or heralded parametric down-conversion (PDC) sources, perform almost as good as single-photon sources. Among the multitude of DQKD experimental techniques proposed in the literature, the technique described in [5], allows one to achieve the desired characteristics of DQKD, with a reduced cost and leading to a robust system. This technique amounts to what communication Engineers would refer to as Pulse Position Modulation (PPM), which allows the use of extremely simple measurements (the time of arrival of a pulse).

Coherent States

In the protocol mentioned above, Alice transmits attenuated coherent states (i.e., modulated pulses of a CW[7] laser) to Bob. Coherent states, representing electromagnetic radiation produced by physical devices such as lasers, are an important class of states for optical communications. It has been shown [43] that the coherent states of a single mode of radiation $|\alpha\rangle$ can be expressed in the form of a superposition of orthonormal eigenstates $|n\rangle$, known as the number of eigenstates:

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{5.13}$$

[6]If a pulse contains more than one photon, then Eve can split off the extra photons and transmit the remaining single-photon to Bob. This is the basis of the photon number splitting attack [42], where Eve stores these extra photons in a quantum memory until Bob detects the remaining single-photon and Alice reveals the encoding basis. Eve can then measure her photons in the correct basis and obtain information on the key without introducing detectable errors.

[7]Continuous wave

Each number eigenstate $|n\rangle$ contains n photons, and hence the probability of obtaining exactly n photons as the outcome of an experiment can be computed as

$$p(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n} \tag{5.14}$$

The number of photons n is therefore Poisson distributed, with average number of photons equal to $E\{\{n\}\} = N_c = |\alpha|^2$.

DQKD using PCD

Alice transmits coherent states to Bob that either she prepares with a mean photon number N_c, or block with the transmission of vacuum pulses. The *k-th* logical bit will be encoded in a two pulse temporal sequence as follows:

$$|0_k\rangle = |\sqrt{N_c}\rangle_{2k-1}|0\rangle_{2k} \tag{5.15}$$

$$|1_k\rangle = |0\rangle_{2k-1}|\sqrt{N_c}\rangle_{2k} \tag{5.16}$$

The time of arrival allows an unambiguous discrimination of the logical qubit. In order to check the presence of an eventual eavesdropper Alice, with a small frequency f, transmits a decoy state.

$$|d_k\rangle = |\sqrt{N_c}\rangle_{2k-1}|\sqrt{N_c}\rangle_{2k} \tag{5.17}$$

Due to the coherence of the laser, the two component of the decoy state have a precise phase relation and thus they always exit a specific gate of an interferometer at Bob's side preceded by an unbalanced Beam Splitter (BS). Such correlation also exists across the boundary between two alternating bits as well. After measurements, Bob announces when the detector after interferometer clicked (set 1, bits for the check) and when the detector at the other exit of BS clicked (set 2, bits to be used for the key reconstruction). The effect of eavesdropping is a breaking of coherence and can be estimated by the measurement of the set 1. After this test, Alice and Bob run error correction and privacy amplification on set 2 thus obtaining the key.

Once the decoy states have been identified and erased from the useful transmitted sequence, the equivalent channel model is simply that of a binary symmetric channel with bit error probability equal to the quantum bit error rate Q, presented earlier in Figure 5.7.

BIMO Quantum Channel

Let N be the theoretical number of photons transmitted for every information bit, while N_{max} corresponds to the maximum number of photons that can be detected in one symbol interval with a positive sign associated to the transmission or reception of a logic-0, and with a negative sign associated to the transmission or reception

of a logic-1. The discrete quantum channel in a QKD system that uses weak laser pulses can be modeled as shown in Figure 5.11 with an input random variable X_w which at the generic k-th instant may assume the values $X_{w_k} \in (-N, +N)$ and an output random variable Y_w which at the generic k-th instant may assume the values $Y_{w_k} \in (-N_{max},...,-2,-1,0,1,2,...,N_{max})$, where $N_{max} \geq N$. The correspnding channel model is denoted as Binary Input Multiple Output (BIMO).

Note that the model below is associated with transmission of one information bit which corresponds to two time slots (hence, the positive-negative designation in the probabilistic channel model), even though the number of photons detectable in a given slot is obviously only a positive quantity.

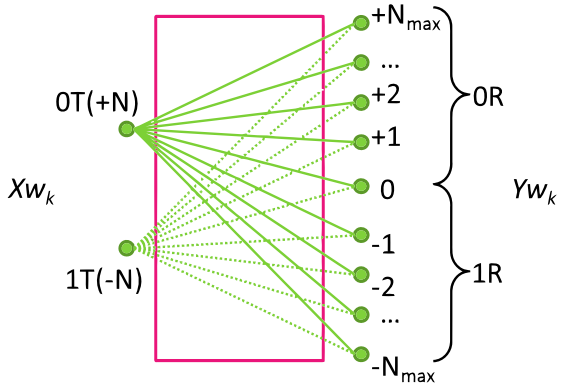


Figure 5.11: Equivalent model for the multi-photon quantum channel when WLP are used

In the case of WLP transmission, soft information can be extracted, as previously discussed. In this case, the soft likelihood metrics will depend on the optical setup used, but in general they are given by the following expressions:

$$LLR(Y_{w_k}) = log\left[\frac{p(Y_{w_k}|X_{w_k}=1)}{p(Y_{w_k}|X_{w_k}=0)}\right] \tag{5.18}$$

that can be expressed as

$$LLR(Y_{w_k}=Y_w(j)) = log\left[\frac{p(Y_{w_k}=Y_w(j)|X_{w_k}=1)}{p(Y_{w_k}=Y_w(j)|X_{w_k}=0)}\right] \tag{5.19}$$

where X_{w_k} are the transmitted bits.

5.5 Soft-Processing of Mixed Metrics

Soft metric processing will be used for error correction and privacy amplification, exploiting all the information available from the detectors at the output of the

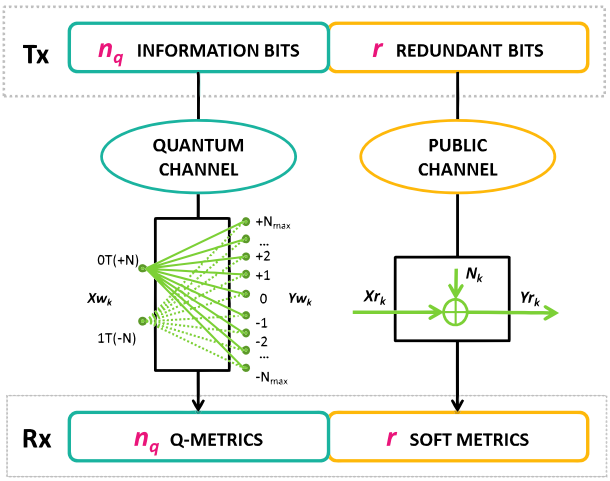


Figure 5.12: Available bits and metrics from the public and the quantum-BIMO channels

public and the quantum channels. This corresponds to using in the post processing algorithms not only the raw received information and redundancy bits, but all the soft information extracted from the channels, i.e., the log-likelihood ratios or LLRs derived from the Equation 5.2, also denoted soft metrics. It is important to remember that the available metrics are derived from two different channels, a "hard output" one and a "soft output" one.

The suggested scheme allows for joint use within the same soft-decoding algorithm of mixed metrics derived from two different equivalent channels. In particular, the public channel offers signal levels typically very reliable, while the quantum channel offers unreliable values. However, in spite of their typically low reliability, it is important to consider them, since they are directly associated to the information bits. In order to determine the perfect combination between soft and hard metrics, a weighed soft metric $\alpha_Q LLR(Y_{p_k})$ has been considered, with $0 \leq \alpha_Q \leq 2$, and the optimal weighing factor α_Q has been determined via simulation, as it will be shown shortly.

Once the appropriate soft (quantized on more than 1 bit) metrics have been associated with the various (information and redundant) bits, the situation is as depicted in Figure 5.13, and a soft metric based block decoder must be identified. As previously discussed, Low Density Parity Check (LDPC) codes provide a viable solution.

Considering one of the results of Shannon's theorem in Forward Error Correction (FEC) channel coding, which indicates that the longer the considered block length the larger its minimum distance and/or the higher its rate, it is convenient to use a very large block length $n_q + r$, which can pose huge constraints on the decoding

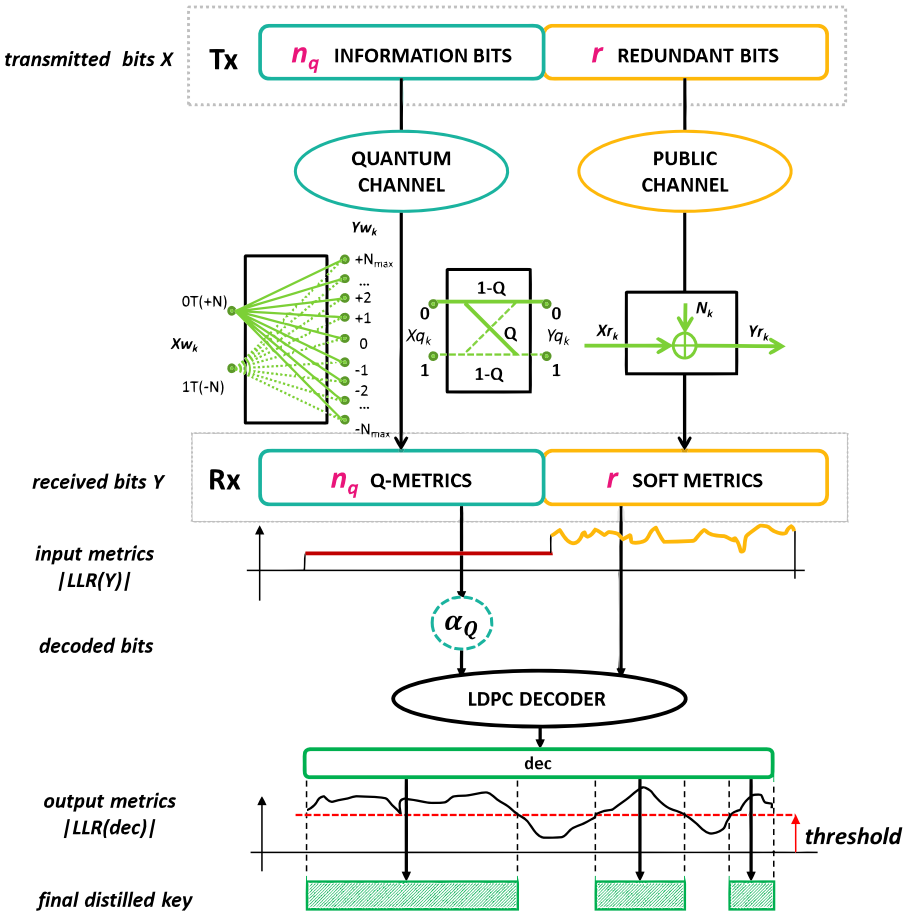


Figure 5.13: Available bits and metrics at transmitter (Alice) and receiver (Bob) for Information Reconcicliation and Pre-Privacy Amplification

complexity. To overcome this, LDPC codes provide a viable solution. In contrast to many classic codes, LDPC codes allow very fast iterative probabilistic decoding algorithms in addition to being a class of linear capacity achieving codes. This makes LDPC codes attractive from both a theoretical and a practical point of view. The use of LDPC codes allows to perform feed-forward information reconciliation, where the errors introduced by the quantum channel are corrected using the redundancy derived from the public channel, without the need to receive further information from the receiver.

Notice that the suggested belief propagation decoding algorithm for LDPC codes offers a "soft" output, which contains not only an estimate of the transmitted bits, but also their reliability, i.e. the amplitude of the output soft metric.

The availability of soft output information, where the decoded bits are paired with the associated reliability, offers an instrument for performing efficient and selective data-sifting and pre-privacy amplification, deleting from the decoded sequence (i.e., form the final distilled quantum key), the bits with low reliability, maintaining the most trusted information, and eliminating residual errors.

As shown in Figure 5.13, the data-sifting and pre-privacy amplification can be performed by comparing the amplitude of the soft metrics associated to the decode bits, with a threshold, and distilling only the bits whose reliability values higher than the threshold.

5.5.1 EXIT Charts for QKD

In Figure 5.14 the block diagram of the LDPC decoder that allows to obtain the EXIT chart of it, is shown within the context of a QKD system. The information transfer for LDPC decoding and the performance of LDPC decoding in the fall-off region can be visualized by the EXIT Chart as said in Chapter 4. It plots the mutual information of the variable nodes decoder versus the mutual information of the check nodes decoder which is modeled by the test (a priori) channel: the output of the yellow branch in Figure 5.14 determines the value of the horizontal axis of the EXIT chart and the output of the blue branch determines the value on the vertical axis.

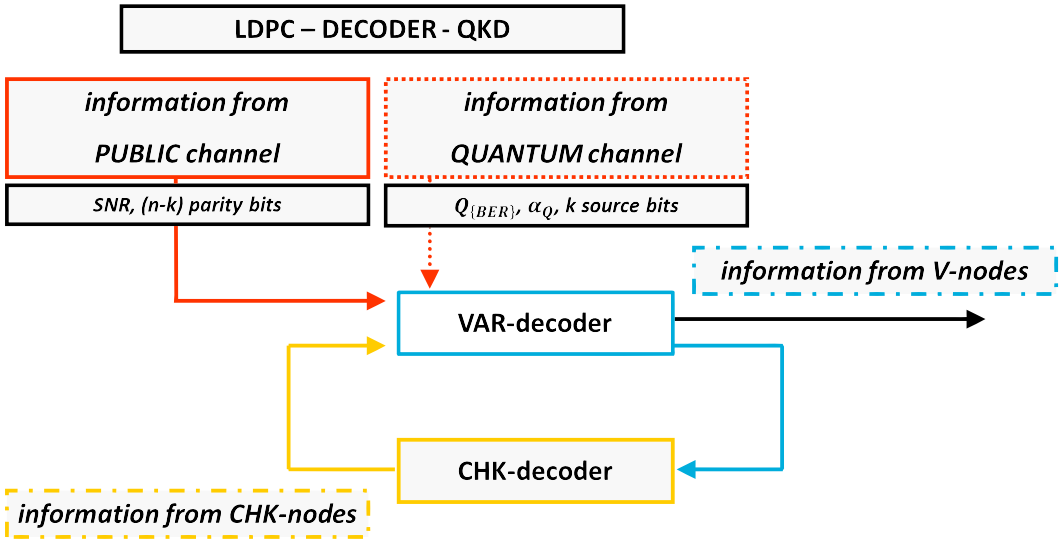


Figure 5.14: EXIT Chart for the LDPC decoder in the context of a QKD system

Chapter 6

Capacity of a Bayesian Quantum Channel employing Photon Counting Detectors

In Chapter 5 the potential improvements in key transmission rate in a Quantum Key Distribution (QKD) scheme whereby photon-counting detectors (PCD) are used at the receiver were discussed. To take full advantage of such detectors, soft information is generated in the form of Log-Likelihood Ratios (LLR's) using a Bayesian estimator of phase of the signal pulse which is used to carry the information.

In this chapter, a feasible scheme suggested in [44] to obtain a soft output quantum channel useful for soft-metric-based information reconciliation protocols for quantum key distribution is studied.

The binary communication scheme proposed in [44] allows to encode the discrete bit values $x_{in} = \{0,1\}$ into an optical polarization qubit, with the advantage that at the detection stage, the output is a real number x_{out}, which can be used for soft-information data processing. In other words, it is possible to obtain a soft output quantum channel to be used, e.g., for quantum key distribution applications such as information reconciliation using FEC. The scheme in based on optical qubits encoded into the polarization degree of freedom of coherent states and Bayesian estimation in non-asymptotic regime at the detection stage, and it is a technique which can operate also in the presence of non dissipative noise during the propagation.

In this chapter the limits of the achievable performance gains when using photon counting detectors are explored and compared to the case when such detectors are not available. To this end, the classical capacity of the Bayesian inference channel is found, clearly showing the potential gains that photon counting detectors can provide in the context of a realistic cost-effective scheme from an implementation point of view. While there are binary communication schemes that can achieve a higher capacity for a given mean photon count at the receiver compared to the

scheme presented here (e.g., the Dolinar receiver), most such schemes are complex and at times unrealistic from an implementation point of view.

6.1 Bayesian Quantum Channel

Figure 6.1 represents a sketch of the binary communication scheme based on the polarization degree of freedom of a coherent state $|\alpha_Q\rangle$ as a qubit and on Bayesian analysis to retrieve the information at the detection stage.

The *k-th* information bit is encoded as $x_{in} = \{0,1\}$ by applying the unitary transformation $U(\varphi_{in})$ to the polarization degree of freedom of a coherent state $|\alpha_Q\rangle$, which is assumed to be initially in the polarization state $|+\rangle = |+45\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$.

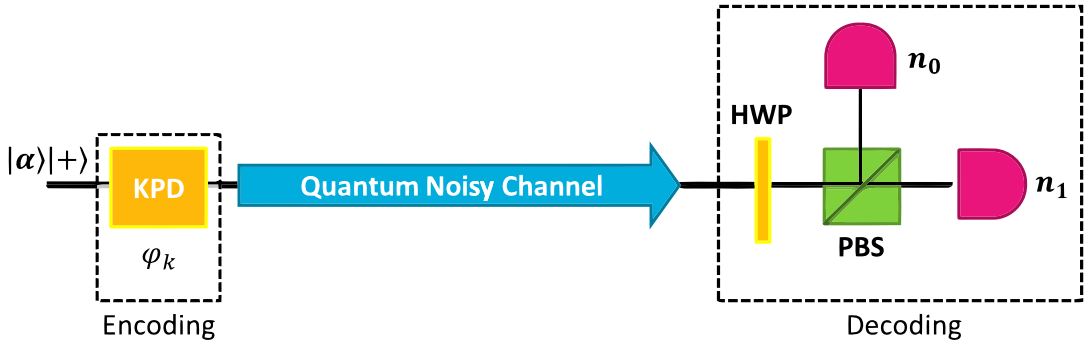


Figure 6.1: A possible experimental setup to generate soft information in QKD applications.

This technique is based on the use of a Phase Beam Splitter (PBS) and two photon counters. The scheme allows to map the discrete bit value x_{in} to an optical polarized qubit, but at the detection stage can produce a discrete set of real numbers, either in the form of Log-Likelihood Ratios, or in the form of output phase values, which can be used for soft information processing. The experimental setup is shown in Figure 6.1, where the polarization degree of freedom of a coherent state φ_{in} is associated to the information bit $|\alpha_Q\rangle$ according to the following encoding rule:

x_{in}	→	φ_{in}
0	→	$\pi/4$
1	→	$3\pi/4$

Figure 6.2: Bayesian Quantum Channel: Encoding rule

where the bit $x_{in} = 1$ has an associated phase shift of $\pi/2$ relative to the bit $x_{in} = 0$. At the detection stage a measurement of the phase shift of the qubit needs

to be performed. This can be implemented as depicted in Figure 6.1 by using a half-wave plate (HWP) placed in front of a polarizing beam splitter (PBS) with two photon-counters providing the number of photons in the reflected and transmitted beams denoted n_0 and n_1 respectively. Let $N_{tot} = n_0 + n_1$ denote the total number of detected photons. It will be assumed that this is also the total number of transmitted photons (in the hypothesis that no photon is lost), which is a Poisson distributed random variable with mean value[1] $N_c = |\alpha_Q|^2$.
From the knowledge of the photon counts $n_0 + n_1$, the actual value of the phase shift can be obtained by using the Bayesian estimator described in [1,2]

$$\varphi_{est} = \int_0^{\pi} \varphi p_B(\varphi|n_0,N_{tot})d\varphi = E\left\{\varphi|n_0,N_{tot}\right\}, \tag{6.1}$$

where,

$$p_B(\varphi|n_0,N_{tot}) = \frac{p(x_{in}=0|\varphi)^{n_0}p(x_{in}=1|\varphi)^{n_1}}{N} = \frac{p(0|\varphi)^{n_0}p(1|\varphi)^{N_{tot}-n_0}}{N} \tag{6.2}$$

is the probability density function of the received phase shift given the fact that N_{tot} photons have been received and n_0 photons have been counted at the "0" output of the PBS, and N is a normalization factor such that

$$\int_0^{\pi} p_B(\varphi|n_0,N_{tot})d\varphi = 1.$$

6.2 Evaluation of the Log-Likelihood Ratios

In soft-decoding algorithms, Log-Likelihood-Ratios are typically required, which in this case can be defined as:

$$LLR\left(n_0,n_1\right) = log\left[\frac{p\left(1 \mid \{n_0,n_1\}\right)}{p\left(0 \mid \{n_0,n_1\}\right)}\right] \tag{6.3}$$

where,

$$p\left(k \mid \{n_0,n_1\}\right) = p\left(\varphi_k \mid \{n_0,n_1\}\right) \qquad k = 0,1 \tag{6.4}$$

is the probability that the transmitted bit was $''k''$ given the measurement pair $\{n_0,n_1\}$. Using Bayes' Theorem, Equation 6.17 can be rewritten as:

$$LLR\left(n_0,n_1\right) = \log\left[\frac{p\left(\{n_0,n_1\} \mid 1\right)}{p\left(\{n_0,n_1\} \mid 0\right)}\right] \tag{6.5}$$

Since coherent states are being used, the number of photons measured at the two detectors are uncorrelated and, in particular, are distributed according to a Poisson

[1] Mean value of a coherent state, see Chapter 5

statistic. Given φ_k, the average number $N_k^{(h)}$ of detected photons at the detector $''h''$ is given by the expression:

$$N_k^{(h)} = N_c \; p\left(h \mid \varphi_k\right) \qquad h,k = 0,1$$

where $N_c = |\alpha_Q|^2$ is the average number of photons of the input coherent state, and

$$p\left(0 \mid \varphi_k\right) = \frac{1}{2}\left(1 + e^{-\Delta^2}\cos\left(\varphi_k\right)\right) \tag{6.6}$$

$$p\left(1 \mid \varphi_k\right) = \frac{1}{2}\left(1 - e^{-\Delta^2}\cos\left(\varphi_k\right)\right) \tag{6.7}$$

where, to make the analysis more general, it is assumed that during propagation, the qubit undergoes a phase diffusion process whose amplitude is characterized by the parameter Δ. The feasibility of this scheme and its experimental demonstration have been thoroughly investigated in [45], including the effect of phase diffusion. Therefore:

$$p\left(\{n_0,n_1\} \mid k\right) = \; \mathcal{P}\left(n_0,N_k^{(0)}\right)\mathcal{P}\left(n_1,N_k^{(1)}\right) \tag{6.8}$$

where,

$$\mathcal{P}\left(n\;,N\right) = \frac{e^{-N}N^n}{n!} \tag{6.9}$$

is the Poisson probability distribution. Then, the following expression for the LLR can be easily obtained:

$$LLR(n_0,n_1) = \log\left\{\frac{p(0|\varphi_1)^{n_0}p(1|\varphi_1)^{n_1}}{p(0|\varphi_0)^{n_0}p(1|\varphi_0)^{n_1}}\right\} \tag{6.10}$$

$$LLR(n_0,n_1) = n_0\log\left[\frac{p\left(0|\varphi_1\right)}{p\left(0|\varphi_0\right)}\right] + n_1\log\left[\frac{p\left(1|\varphi_1\right)}{p\left(1|\varphi_0\right)}\right] \tag{6.11}$$

Considering that $\varphi_0 = \frac{\pi}{4}$ and $\varphi_1 = \frac{3\pi}{4}$, further simplifications can be made:

$$p\left(0|\varphi_0\right) = \frac{1}{2}\left(1 + e^{-\Delta^2}\cos\left(\varphi_0\right)\right) = \frac{1}{2}\left(1 + e^{-\Delta^2}\cos\left(\frac{\pi}{4}\right)\right)$$

$$p\left(1|\varphi_0\right) = \frac{1}{2}\left(1 - e^{-\Delta^2}\cos\left(\varphi_0\right)\right) = \frac{1}{2}\left(1 - e^{-\Delta^2}\cos\left(\frac{\pi}{4}\right)\right)$$

$$p\left(0|\varphi_1\right) = \frac{1}{2}\left(1 + e^{-\Delta^2}\cos\left(\varphi_1\right)\right) = \frac{1}{2}\left(1 + e^{-\Delta^2}\cos\left(\frac{3\pi}{4}\right)\right) = \frac{1}{2}\left(1 - e^{-\Delta^2}\cos\left(\frac{\pi}{4}\right)\right)$$

$$p\left(1|\varphi_1\right) = \frac{1}{2}\left(1 - e^{-\Delta^2}\cos\left(\varphi_1\right)\right) = \frac{1}{2}\left(1 - e^{-\Delta^2}\cos\left(\frac{3\pi}{4}\right)\right) = \frac{1}{2}\left(1 + e^{-\Delta^2}\cos\left(\frac{\pi}{4}\right)\right)$$

It can be seen that the first two and the last two equations are equivalent respectively, therefore a transmission and a transition probability can be defined, given by the following expressions:

$$p_{ii} = p\,(0|\varphi_0) = p\,(1|\varphi_1) \tag{6.12}$$

$$p_{ij} = p\,(0|\varphi_1) = p(1|\varphi_0) \tag{6.13}$$

where:

$$p_{ii} = 1 - p_{ij} \tag{6.14}$$

Replacing the expressions for p_{ii} and p_{ij} in Equation 6.9, the following expression can be obtained:

$$LLR\,(n_0,n_1) = \log\left[\frac{p_{ij}^{n_0} p_{ii}^{n_1}}{p_{ii}^{n_0} p_{ij}^{n_1}}\right] \; = log\left[p_{ij}^{n_0-n_1} p_{ii}^{n_1-n_0}\right] \tag{6.15}$$

$$LLR\,(n_0,n_1) = -(n_1 - n_0)\log(p_{ij}) + (n_1 - n_0)\log(p_{ii}) \tag{6.16}$$

Finally, the expression for the LLR's given by Equation 6.9 can be written as:

$$LLR\,(n_0,n_1) = (n_1 - n_0) log\left(\frac{p_{ii}}{p_{ij}}\right) \tag{6.17}$$

6.3 Evaluation of the soft output phase values

In some applications, a normalized soft output phase value may be required, that will be denoted as $x_{out} \in [-1, +1]$. This section is dedicated to derive such a value from the considered Bayesian estimator. An example of the $p_B(\varphi|n_0,N_{tot})$ function is shown in Figure 6.3, for N_{tot}=6 and n_0=0,...,N_{tot}[2].It is possible to observe how the mean value of the received phase shift probability density function moves towards 0 when the number of photons counted at the "0" output n_0 increases, while the mean value moves towards $\pi/2$ when the number of photons counted at the "1" output n_1=N_{tot}-n_0 increases.

The Bayesian estimator φ_{est} generates as estimates, the $N_{tot}+1$ mean values of the $N_{tot}+1$ distributions in Figure 6.3, depending on n_0,. Notice that the estimator is known to be *asymptotically* optimal, that is, it allows the phase estimation with the minimum uncertainty admitted by quantum mechanical laws (the quantum Cramer-Rao bound)[46] when the number of counted photons N_{tot} becomes very large. In the current application, however, the interest is focused on a possibly "shot-by-shot" observation, far from the asymptotic regime. To obtain a rough but reliable and simpler estimation of the phase shift, the following estimator can be used:

[2]For a phase diffusion parameter $\Delta = 0.1$

$$\varphi_{out} = \{\varphi_M | p_B(\varphi_M | n_0, N_{tot}) \geq p_B(\varphi | n_0, N_{tot}), \forall \varphi \in [0, \pi]\} \tag{6.18}$$

whereby the detector output phase is the mode of the density function instead of its mean value. Notice that φ_{out} always exists and it is unique. Of course, as the total number of detected photons $n_0 + n_1$ increases, φ_{out} and φ_{est} come to coincide [47] [45]. The $N_{tot}+1$ values of φ_{out} derived from Figure 6.3 are shown in Figure 6.4 as a function of n_0.

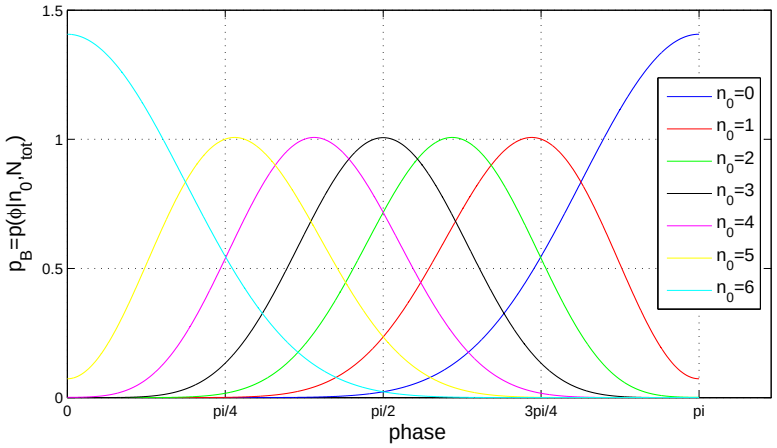


Figure 6.3: The normalized functions $p_B(\varphi|n_0,N_{tot})$ for N_{tot}=6

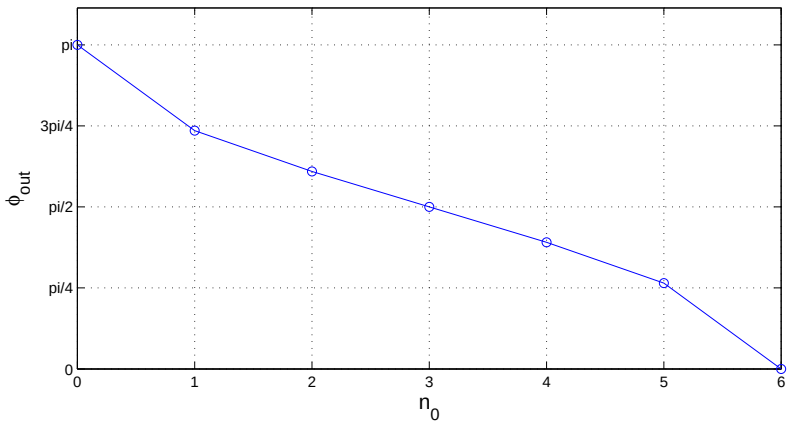


Figure 6.4: The $N_{tot}+1$ values of φ_{out} obtained for $N_{tot} = 6$ as a function of n_0=6

Once the value φ_{out} has been estimated, a real value for x_{out} can be obtained via

the transformation:

$$x_{out} = \frac{2}{\pi}\left(\varphi_{out} - \frac{\pi}{2}\right) \tag{6.19}$$

Note that $x_{out} \in [-1, +1]$ is represented on $N_{tot}+1$ levels. The soft output levels (not to be confused with LLR values) obtained for N_{tot}=6 are shown in Figure 6.5 as a function of n_1-n_0.

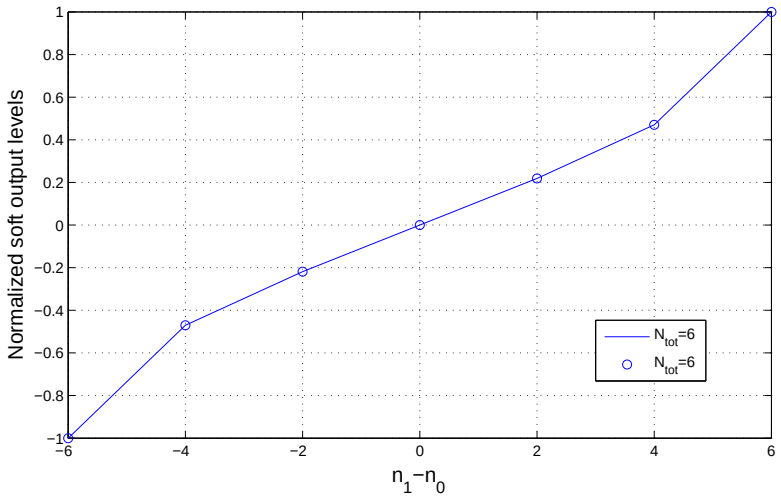


Figure 6.5: Detector characteristics showing the normalized soft output levels obtained for N_{tot}=6 as a function of n_1-n_0

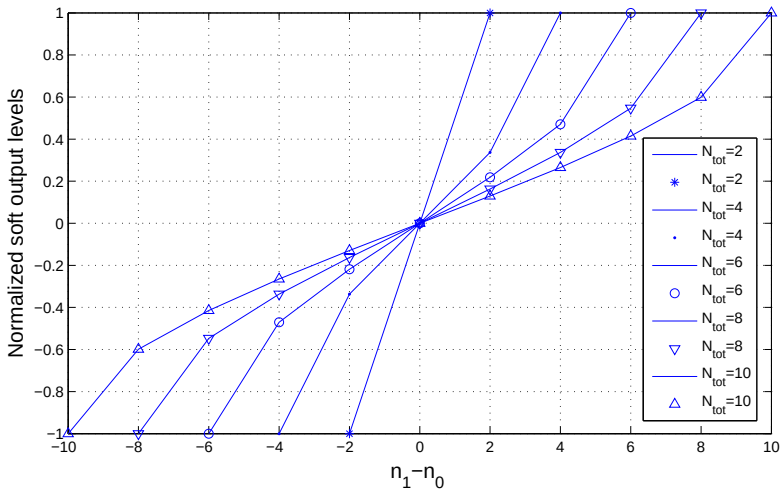


Figure 6.6: Detector characteristics (normalized soft output value of level as a function of n_1-n_0) for N_{tot}=2,4,6,8,10

The detector characteristics, offering the $N_{tot}+1$ values of x_{out} for $N_{tot}=2,\ldots,10$ are shown in Figure 6.6.

Notice that, although the output range is constant, the achievable resolution available in the representation of the normalized output x_{out} increases with the number of received photons.

6.4 Capacity Evaluation

The quantum channel in d-dimensions is often modeled as a completely positive trace preserving map Ψ. The most common channel model is the depolarizing channel which depends on one parameter λ mapping a mixed state in C^d into:

$$\rho \;\rightarrow\; \lambda\rho + \frac{1-\lambda}{d}\, I$$

Where, I is the $d \times d$ identity matrix. For a general quantum channel, let ε denote the ensemble of input states, and M the measurement or a Positive Operator Valued Measure (POVM)[3] $\{\mathrm{E}_j\}$ at the channel output. The input state ensemble, channel and measurement together define a classical noisy channel with probability transitions:

$$p_{nm} = Tr[\Psi\left(\rho_{\mathrm{n}}\right)\mathrm{E}_{\mathrm{m}}]$$

Defining the probabilities over the input state, which we will denote as X, a natural definition of classical capacity of the quantum channel would be:

$$C_{shan}\left(\Psi\right) = \sup_{\varepsilon,\mathrm{M}} \;\; \mathrm{I(X,Y)}$$

where I(X,Y) is the Shannon mutual information. The complication in defining capacity of the quantum channel in contrasts with the classical channel really arises in connection with purely quantum mechanical effects which have no analogue in the classical domain, i.e., entanglement[4]. In particular, in general it is reasonable to assume (which is in fact shown to be true) that the capacity of parallel copies of a quantum channel with entangled inputs may be larger than the sum capacity of each channel treated separately. It turns out that for the most common channel model, namely the depolarizing channel, entanglement buys nothing.

The closest analogue of the binary communication scheme proposed in this chapter is Binary Phase Shift Keying (BPSK) using coherent states. It is well known

[3]POVM (Positive Operator Valued Measure) is a measure whose values are non-negative self-adjoint operators on a Hilbert space. It is the most general formulation of a measurement in the theory of quantum physics.

[4]Quantum entanglement occurs when particles such as photons, electrons, and some other particular molecules interact physically and then become separated; the type of interaction is such that each resulting member of a pair is properly described by the same quantum mechanical description (state), which is indefinite in terms of important factors such as position, momentum, spin, polarization, etc.

that for such a scheme the Dolinar receiver achieves nearly optimal results with capacity:

$$C_{BPSK-Dolinar} = 1 - H_2\left(0.5(1 - \sqrt{1 - e^{-4N_C}})\right)$$

where, $H_2(.)$ is the binary Entropy function. This capacity is close to the ultimate capacity obtained using an as yet unknown optimal receiver:

$$C_{BPSK-Ultimate} = 1 - H_2\left(0.5(1 + e^{-2N_C})\right)$$

The Dolinar receiver requires a complicated feedback system for its implementation. Hence, while its capacity for a given N_c is greater than what is reported here, there is significant difference in the level of the complexity of the receiver.

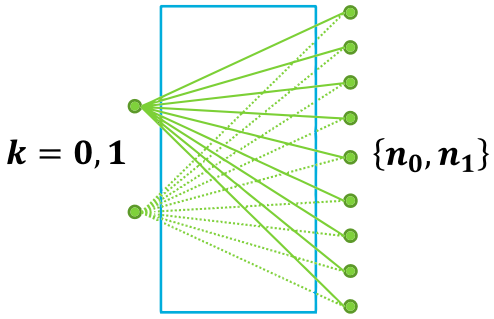


Figure 6.7: BIMO DMC Quantum Channel

The discussion thus far has been general and focused on quantum channels as trace-preserving maps. In this section, however, is focused on a more humble pursuit, which is that of modeling an experimental setup using realistic off-the-shelf components and a particular method of communicating the quantum states, and specifically calculating the traditional Shannon capacity of the link viewed as a probabilistic transition mechanism that maps input bits into possibly multi-level signals used for detection. In this sense, the quantum channel is modeled as a Binary Input Multilevel Output (BIMO) Discrete Memoryless Channel (DMC), and the main goal of this section is to contrast the capacity of a system employing photon counting detectors to that of the equivalent Binary Symmetric Channel (BSC) resulting from reducing the photon counts into presence or absence of signals (i.e., hard decoding).

As noted earlier, the sufficient statistic for detection with photon counting detectors is the count difference of detector 1 and 0, i.e., (n_1-n_0). Since each variable is an independent Poisson random variable, the difference (n_1-n_0) is Skellam distributed:

$$n_1 \sim Poisson,\ \mu_1 = N_k^{(1)} \tag{6.20}$$

$$n_0 \sim Poisson,\ \mu_0 = N_k^{(0)} \tag{6.21}$$

$$P\left(n_1\text{-}n_0{=}m \mid \varphi_k\right) = e^{-\left(N_k^{(1)}+N_k^{(0)}\right)} \left(\frac{N_k^{(1)}}{N_k^{(0)}}\right) I_{|m|} 2\sqrt{\left(N_k^{(1)}.N_k^{(0)}\right)} \tag{6.22}$$

where, *k=0 or 1*, and $\mathrm{I}_{|m|}(.)$ is the modified Bessel function of the first kind and order $|m|$.

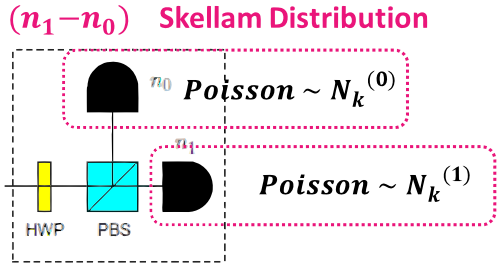


Figure 6.8: Decoding stage: Skellam distribution $(n_1\text{-}n_0)$

Note that m itself is an integer that can be positive or negative. Plugging known values of the parameters, the following expression can be obtained:

$$N_k^{(0)} + N_k^{(1)} = N_c \tag{6.23}$$

$$\frac{N_k^{(1)}}{N_k^{(0)}} = \frac{p(1|\varphi_k)}{p(0|\varphi_k)} \tag{6.24}$$

$$N_k^{(1)} \cdot N_k^{(0)} = {N_c}^2 p(1|\varphi_k) p(0|\varphi_k) \tag{6.25}$$

Specializing to the case "zero is transmitted and is mapped to φ_0" it is possible to derive the following expression:

$$P(n_1\text{-}n_0{=}m|\varphi_0) = e^{N_c} \left(\frac{\sqrt{2}-e^{-\Delta^2}}{\sqrt{2}+e^{-\Delta^2}}\right) I_{|m|}\sqrt{N_c\sqrt{1-\frac{e^{-2\Delta^2}}{2}}}$$

and similarly for the case "one is transmitted and is mapped to φ_1" :

$$P(n_1\text{-}n_0{=}m|\varphi_1) = e^{N_c} \left(\frac{\sqrt{2}+e^{-\Delta^2}}{\sqrt{2}-e^{-\Delta^2}}\right) I_{|m|}\sqrt{N_c\sqrt{1-\frac{e^{-2\Delta^2}}{2}}}$$

Let X be the random variable associated with the transmitted phase and Y be the channel output which is our sufficient statistic $(n_1\text{-}n_0)$. Then, the formulas above give the expression for the channel transition probabilities for the DMC. Using the classic definition of mutual information:

$$I\left(X,Y\right) = H\left(X\right) - H\left(X \mid Y\right) \tag{6.26}$$

and noting that the input is binary with $p(X{=}0){=}p(\varphi_0){=}p$, after some manipulation we have:

$$p(X{=}0|Y{=}m) = \frac{p}{p\,(1-\alpha_{Q_\Delta}^{m}) + \alpha_{Q_\Delta}^{m}} \tag{6.27}$$

$$p(X{=}1|Y{=}m) = \frac{(1-p)\alpha_{Q_\Delta}^{m}}{p\,(1-\alpha_{Q_\Delta}^{m}) + \alpha_{Q_\Delta}^{m}} \tag{6.28}$$

where,

$$\alpha_{Q_\Delta} = \frac{\sqrt{2}+e^{-\Delta^2}}{\sqrt{2}-e^{-\Delta^2}} \tag{6.29}$$

Finally, the conditional entropy based on two parameters, p and Δ can be written as:

$$\begin{aligned} H(X|Y) = &-e^{-N_c}\sum_{m} p\left(\frac{1}{\alpha_{Q_\Delta}}\right)^{\frac{m}{2}} I_{|m|}\left(\sqrt{N_c\sqrt{1-\frac{e^{-2\Delta^2}}{2}}}\right) log(p(X{=}0|Y{=}m)) \\ &-e^{-N_c}\sum_{m} (1-p)\left(\alpha_{Q_\Delta}\right)^{\frac{m}{2}} I_{|m|}\left(\sqrt{N_c\sqrt{1-\frac{e^{-2\Delta^2}}{2}}}\right) log(p(X{=}1|Y{=}m)) \end{aligned} \tag{6.30}$$

While the BIMO DMC is neither symmetric nor weakly symmetric, it is not difficult to show that the maximizing input probability distribution is uniform. Hence, *p=0.5* maximizes the mutual information leading to channel capacity. To compare the capacity of the link employing photon counting detector to that of a simple detector signaling the presence or absence of signal, we need to specify how such a detector behaves. It is logical to assume that cross-over probability of the BSC channel associated with such a receiver can be obtained via:

$$p_{BSC} = \sum_{m=1}^{\infty} P(n_1\text{-}n_0{=}m|\varphi_0) + \frac{1}{2}P(n_1\text{-}n_0{=}0|\varphi_0) \tag{6.31}$$

Notice that when $(n_1\text{-}n_0){=}0$ (which for low values of N_c happens often), the detector chooses at random between *k=0* and *k=1.*

Figure 6.9 depicts the capacity of the BIMO DMC and its comparison to the equivalent Binary Symmetric Channel (BSC) channel in case of hard decision decoding as a function of the mean photon count in the case the phase diffusion parameter is zero.

Figure 6.10 depicts the capacity of our BIMO DMC and its comparison to the equivalent BSC in case of hard decision decoding as a function of the phase diffusion parameter Δ for three different values of the mean photon count.

It can be observed that the considered BIMO DMC channel offers a capacity improvement over the equivalent BSC. This improvement could lead to a BER improvement when comparing the two channels in presence of an error correction code. This is investigated in the next section.

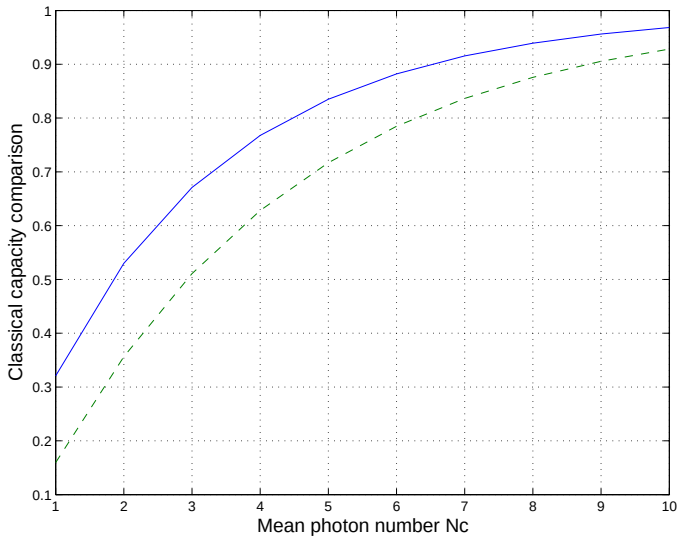


Figure 6.9: Classical capacity of BIMO DMC (solid green curve) compared to the equivalent BSC with transition probability p_{BSC}, as a function of mean photon count Nc.

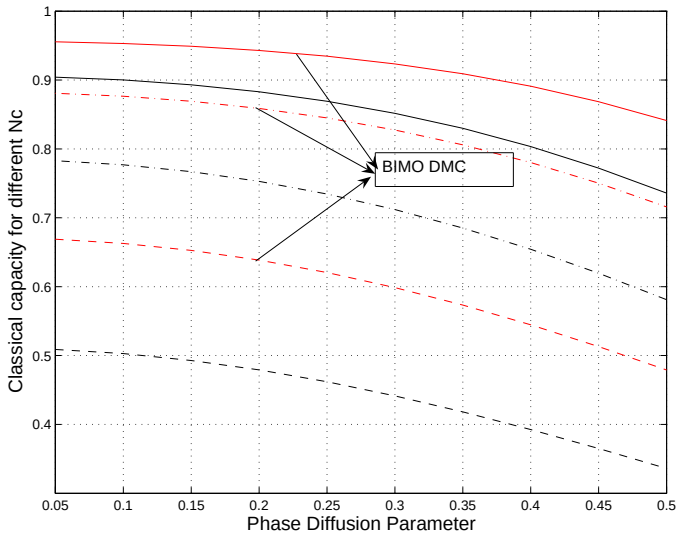


Figure 6.10: Classical capacity of BIMO DMC and equivalent BSC with transition probability as a function of phase diffusion parameter for three different values of Nc (solid line: N_c=9, dash-dot line: N_c=6, dash line: N_c=3).

Chapter 7

Soft-QKD Protocol Performance

In this chapter, the novel protocol for error correction and information reconciliation are validated by means of intensive software simulations under well defined scenarios, and a short description of the software for the simulation of the soft-QKD Protocol proposed in the previous chapters is presented. The soft-QKD simulator is a tool to simulate and analyze the performance of the proposed protocol using different schemes for Quantum Key Distribution. Thus, allows to compare the performance of the proposed soft-metric protocol when applied to different QKD scenarios.

7.1 Simulations Set-up

The Soft-QKD Protocol simulator takes into account the characteristics of the following sub-blocks:

- Quantum communication system: the quantum channel is represented according to one of the models suggested in chapter 5, depending on the corresponding scheme used for quantum transmission and detection. The value of the estimated quantum bit error rate (Q_{BER}) can be selected by the user.
- Public communication system: the public channel is modeled as an AWGN channel, with an elevated signal-to-noise ratio (E_b/N_0), since deep coding is allowed on the public link errors can be neglected. The digital modulation scheme can also be selected by the user.
- LDPC decoder: uses belief propagation techniques, the values of the soft-metrics (LLR's) derived from the two sub-systems that form the composite communication channel, are calculated according to the schemes selected to model each one of them. The bit values and the LLR's values after the quantum and the classical transmission should be passed as an input to the decoder. The number of iterations for decoding can be selected as well as the minimum

number of errors the user intends to correct. The parity matrix of the LDPC code used in the simulator is chosen from a set of suggested codes.

For the presentation of the simulation results, two figures will be used: the BER or Bit Error Rate of the distilled key and the FER or Frame Error Rate of the distilled key. A single frame is equivalent to a decoded code block.

7.2 LDPC Codes Performance

Simulations using LDPC codes with various rates (0.5, 0.61 and 0.75) and various block lengths have been conducted. In Figure 7.1 a comparison between the BER performance of three LDPC codes with rates R_c=0.5,0.617,0.75, decoded with 50 iterations as a function of the ratio (E_b/N_0) on a classic AWGN channel are shown. The codes with rate R_c=0.5 and 0.617 have been selected to conduct further simulations for the soft-QKD protocol, since their performance is better than the code with rate R_c=0.75, and the security of the communication is guaranteed for a rate equal or higher than 0.5. In Figure 7.2, the BER values of a n=n_q+r=408, r=252

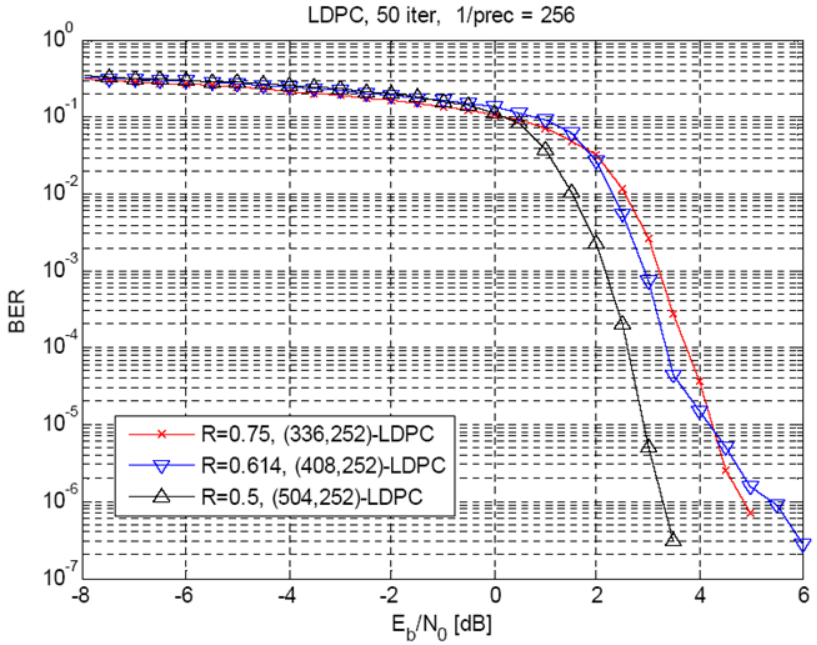


Figure 7.1: Comparison between the BER performance of three LDPC codes with rates R_c=0.5,0.617,0.75, decoded with 50 iterations as a function of (E_b/N_0) on a classic AWGN channel

and R_c=0.5 code are compared with those of a n=n_q+r=1000, r=500 and $Rc = 0.5$ code, one for Q in the range 0.12-0.5, showing that, as expected, longer code blocks (and higher complexity) allow for better decoding performances.

Weighed q-metric values $\alpha_Q LLR(Y_{p_k})$ have been considered. The parameter α_Q has been inserted in order to optimize the contribution of the information derived from the q-bits.

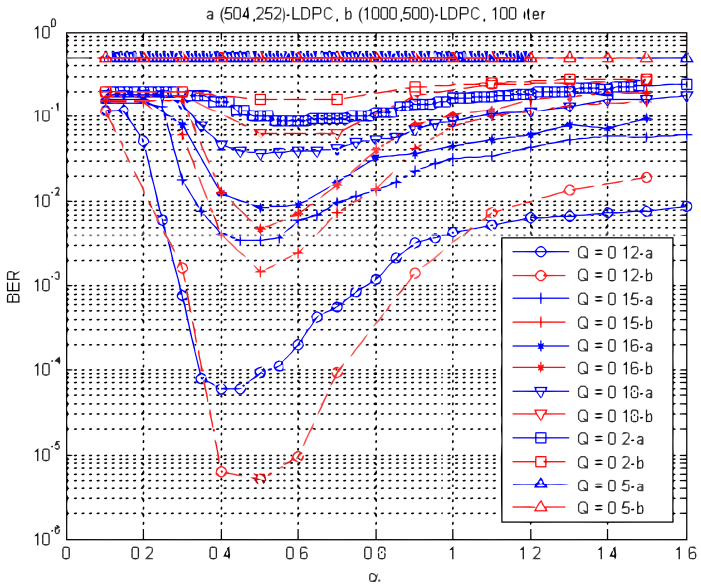


Figure 7.2: Comparison between the BER performance of two LDPC codes with R_c=0.5, one with n=n_q+r=408, r=252 and one with n=n_q+r=1000, r=500 as a function of Q and α.

Now that has been demonstrated that longer code blocks allow for better performance, due to limited computational power, for simulation purposes only LDPC codes with limited lenght will be considered.

7.3 LDPC Codes for QKD

7.3.1 Binary Symmetric Quantum Channel

When the quantum channel is model as a BSC the results presented next have been obtained via simulation. In Figure 7.3 the simulated Bit Error Rate (BER) is reported for an LDPC code with n=n_q+r=504, r=252 and rate R_c=0.5, decoded with 100 iterations, for different values of the Q_{BER} parameter Q in the range 0.1 to 0.5, as a function of the weigh parameter α_Q. It can be observed how an optimal value of α in the order of 0.4 can be identified, which however depends on the Q_{BER} parameter Q. Optimizing α_Q allows for a strong performance improvement, lowering the achievable error rates up to three orders of magnitude. It can also be observed that the decoder performance converges to low BER values only if Q is smaller than roughly 0.15, allowing for reliability control, as described in Chapter 4.

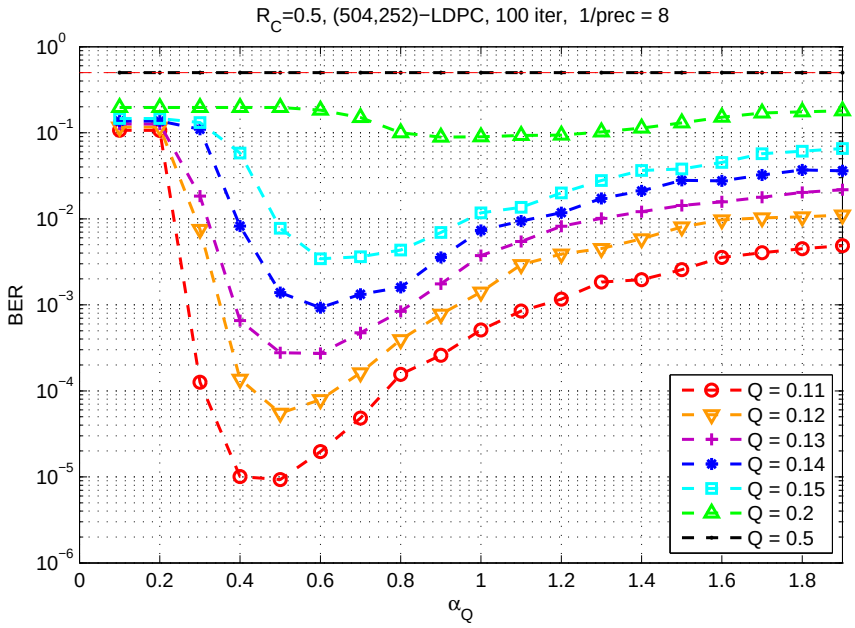


Figure 7.3: BER performance of a LDPC code with n=n_q+r=504, r=252 and R_c=0.5, decoded with 100 iterations as a function of Q and α_Q

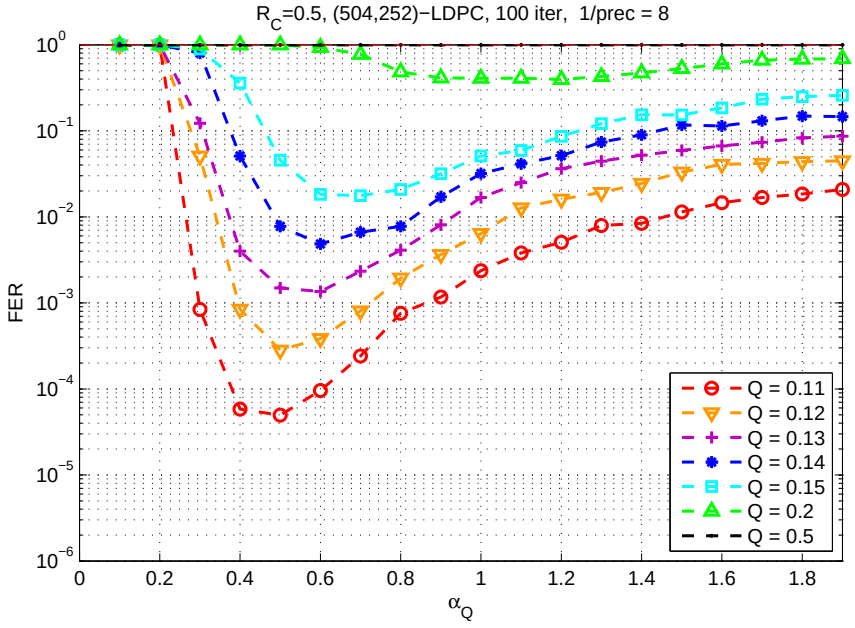


Figure 7.4: FER performance of a LDPC code with n=n_q+r=504, r=252 and R_c=0.5, decoded with 100 iterations as a function of Q and α_Q

In Figure 7.4 the simulated Frame Error Rate (FER) is reported for an LDPC code with n=n_q+r=504, r=252 and R_c=0.5 again, decoded with 100 iterations, for different values of the Q_{BER} as a function of the weigh parameter α_Q. It can be observed how an optimal value of α_Q in the order of 0.5-0.6 can be identified, which however depends always on the Q_{BER} parameter.

Figures 7.5 and 7.6 instead, show the BER and the FER performance respectively, of an LDPC code with n=n_q+r=408, r=252 and R_c=0.61, decoded with 100 iterations as a function of Q and α_Q. The behavior is similar as in Figures 7.3 an 7.4, and the optimal value for α is approximately 0.35 varying for each value of Q_{BER}. The comparison between the BER and FER values for the two LDPC codes considered until now, with rates, $R_c = 0.5$ and $R_c = 0.61$ is shown in Figure 7.7, more specifically, the comparison between the FER for the two selected LDPC codes as a function of the parameters α_Q and Q_{BER} can be seen in Figure 7.8. It can be observed how the R_c=0.5 LDPC code guarantees better correcting capabilities than the $R_c = 0.61$ LDPC code, however this would also diminished the security of the protocol, due to the larger fraction of public bits that needs to be exchanged over the public channel.

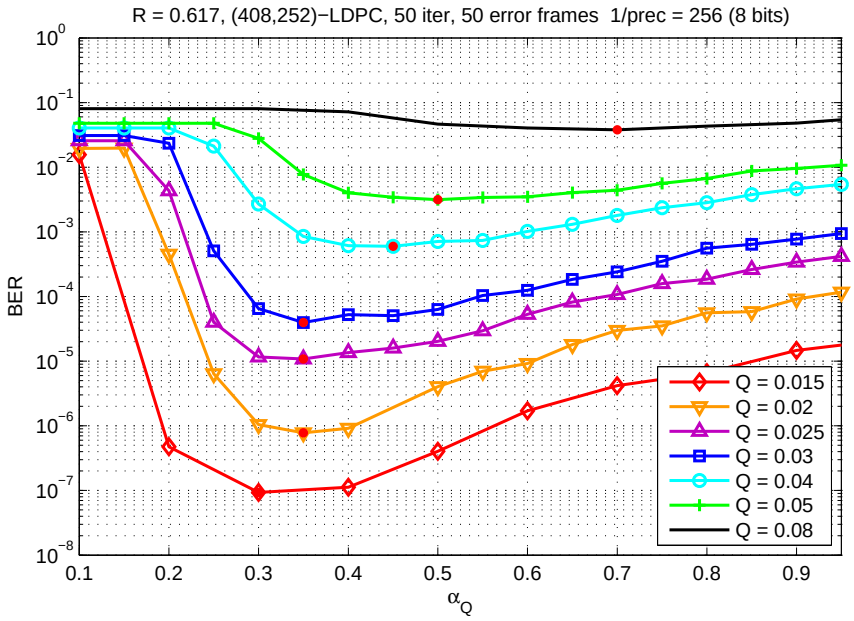


Figure 7.5: BER performance of a LDPC code with n=n_q+r=408, r=252 and R_c=0.61, decoded with 100 iterations as a function of Q and α_Q

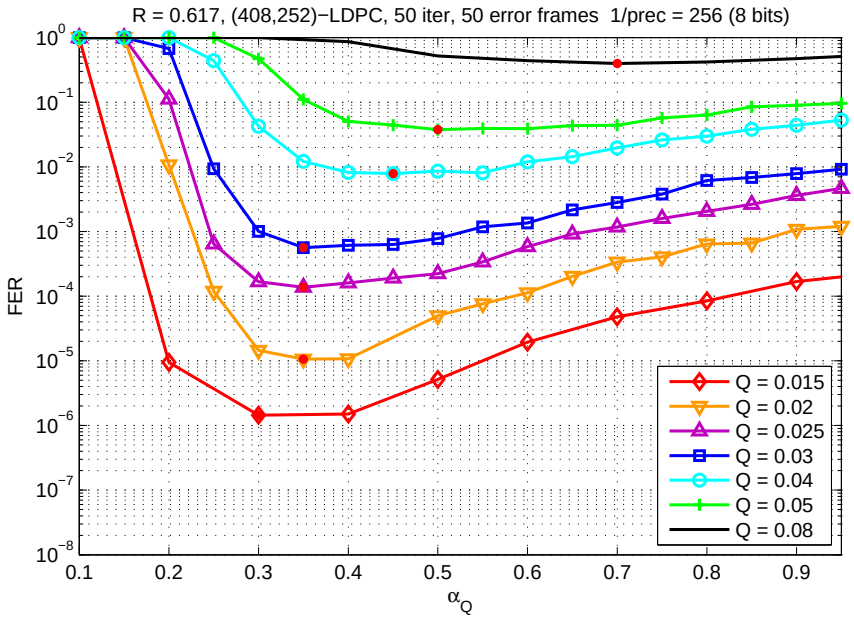


Figure 7.6: FER performance of a LDPC code with n=n_q+r=408, r=252 and R_c=0.61, decoded with 100 iterations as a function of Q and α_Q

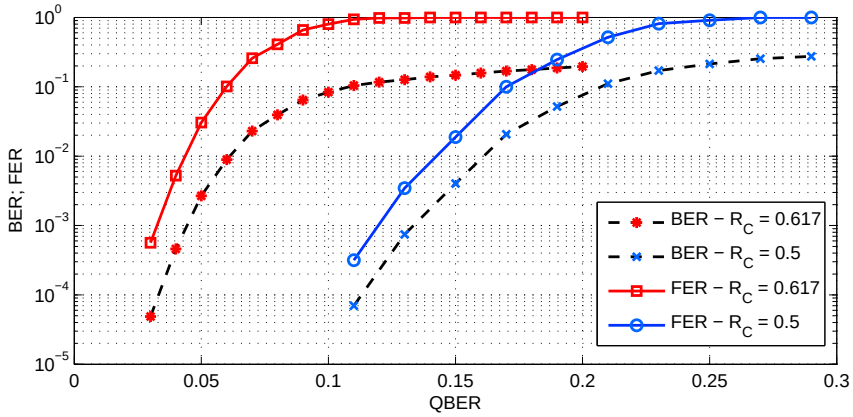


Figure 7.7: BER and FER performance of the LDPC decoders considered in Figures 7.3 and 7.5 as a function of Q for α_Q =1

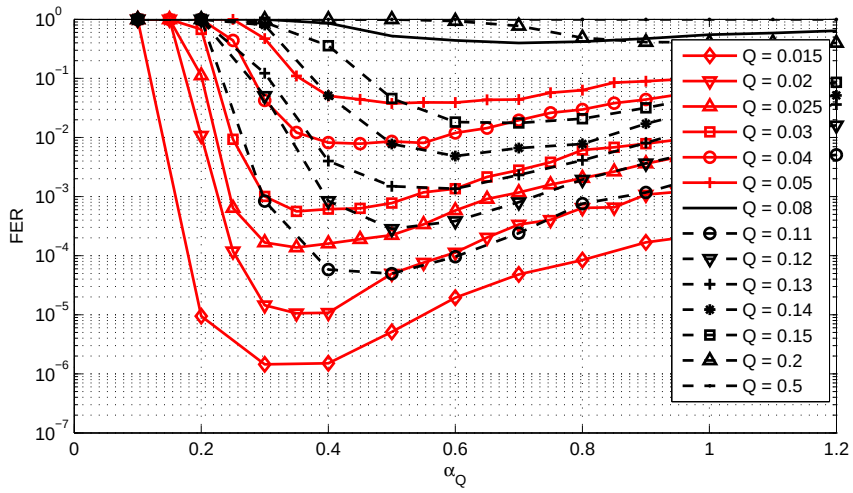


Figure 7.8: FER performance of the LDPC codes with rates R_c=0.5 and R_c=0.61, as a function of Q and α_Q

EXIT Charts

In order to cross-check the presence of an optimal value for the weighting factor α, the EXIT charts of the considered LDPC decoders for α=0.1,0.5,1.5 are shown in Figure 7.9, proving that intermediate values of α_Q (in this case, the value α_Q=0.5) offer open decoding channels, justifying the presence of an optimal value on α_Q in the previous figures. From the EXIT chart evaluated for the LDPC code with R_c = 0.61 depicted for Q = 0.08 and various values of α_Q, it is straightforward to notice that the maximum opening of the decoding tunnel between variable and check nodes decoding curves is achieved for α_Q = 1, in accordance with what observed in Figure

7.6. When the value of α_Q is too small -for instance 0.1- or too large -for instance 1.6- the variable nodes curve intersects the check nodes curve and, consequently, the belief propagation decoder cannot converge to any codeword in the space of possible solutions.

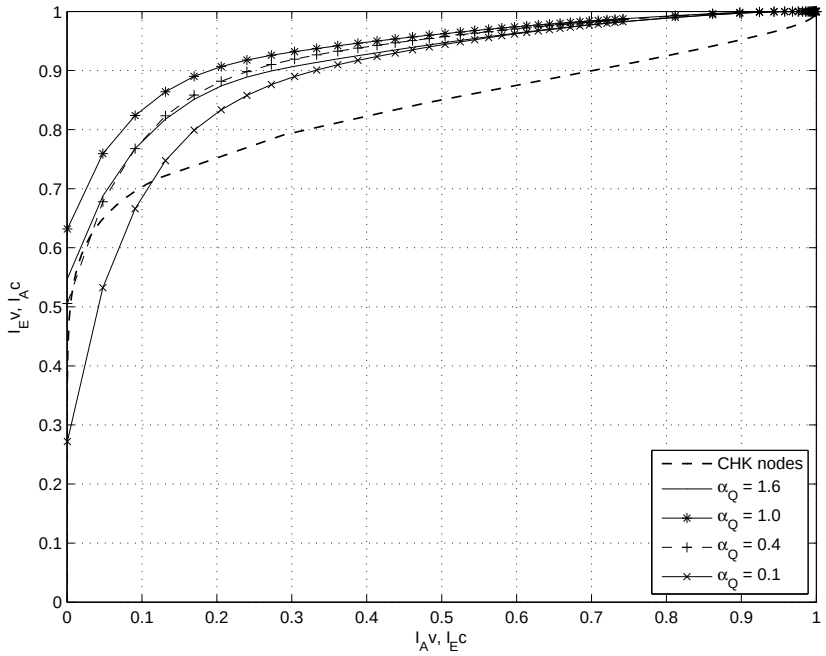


Figure 7.9: EXIT chart of the LDPC decoder considered (lower curve) as a function of α_Q and for $Q = 0.08$

LDPC Decoder Convergence

Figure 7.10 depicts the number of iterations needed to achieve the FER values of Figure 7.6, i.e. for an LDPC code with rate R_c=0.61, showing the strong correlation between FER (and BER) of the decoded sequence and number of iterations. Since the FER/BER of the decoded sequence is typically correlated to the channel Q parameter, the behavior of Figure 7.10 suggests that the number of iterations could be used as a valid indicator of the actual channel Q_BER. Being able to estimate the parameter Q from the decoded bits may allow the detection of a possible eavesdropper without wasting additional bits.

In the next page, Figure 7.11 shows the average number of iterations as a function of the channel Q_{BER} parameter, when α_Q=1 and Q_{est}=0.05, and shows that when the Q_{BER} value increases with respect to the expected value Q_{est}, the decoder tends to converge more slowly. Since the eavesdropping operation increases the Q_{BER} value, detecting an increase in Q_{BER} is equivalent to detecting the presence of Eve.

Figure 7.11 also shows the variance of the number of decoding operations, normalized with respect to the square of its mean value. The fact that the normalized variance decreases with Q shows that the average number of decoding iterations is indeed a good estimator, whose accuracy increases with Q, i.e., when the eavesdropping becomes more relevant.

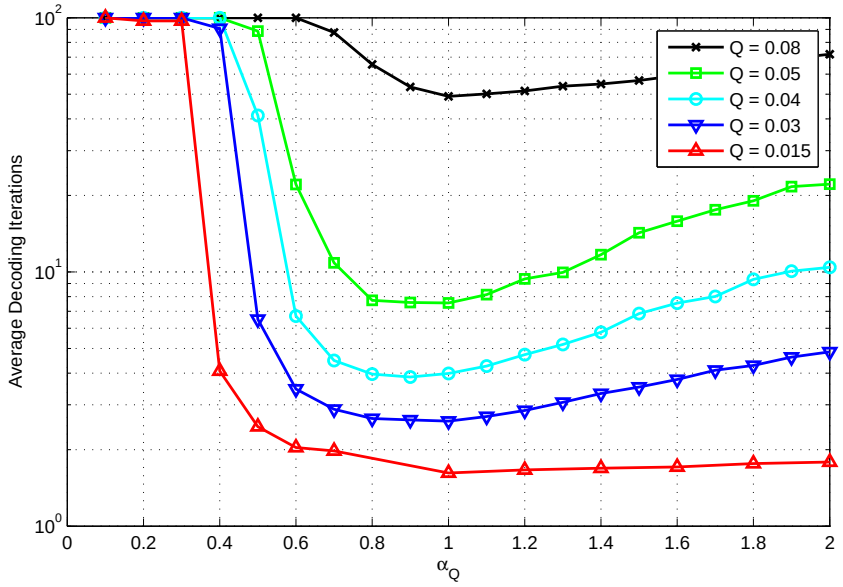


Figure 7.10: Average number of iterations for the LDPC code with R_c= 0.61 as a function of α_Q and for several values of Q_{BER})

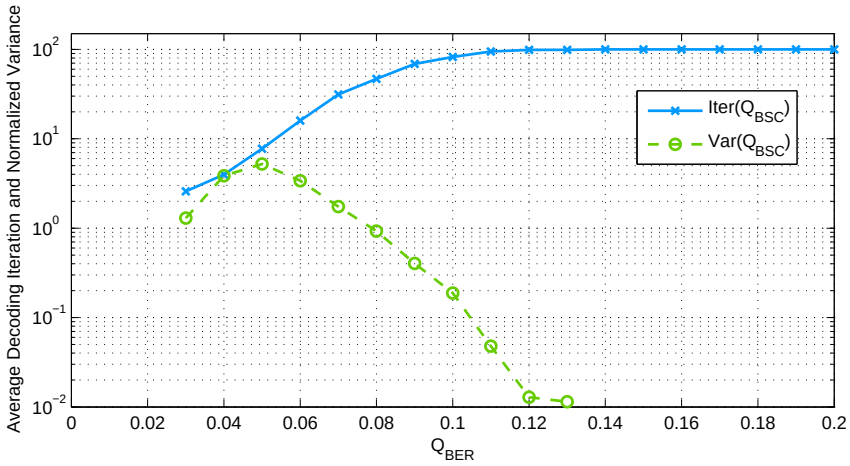


Figure 7.11: Average number of decoding iterations and normalized variance of the number of iterations for the code with Rc=0.61 as a function of Q for $\alpha_Q = 1$ and $Q_{est} = 0.05$

7.3.2 Binary Erasure Quantum Channel

When the lost photons are taken into account, it has been established that the quantum channel can be model as a BEC (Binary Erasure Channel), considering both errors and erasures. In Figure 7.12 the BER simulation results for LDPC codes with rate R_c=0.5(n_q= 504, r = 252) and R_c=0.617(n_q= 408, r = 252) obtained with a private quantum channel model with erasure are shown. BER simulation results for LDPC codes with rate R_c=0.5(n_q= 504, r = 252) and R_c=0.617(n_q= 408, r = 252) obtained with a private quantum channel with erasure are shown, when the erasure channel model is used the corresponding metrics of the erasure bits are considered null, therefore the overall BER worsen when using this model, as can bee seen on Figure 7.12.

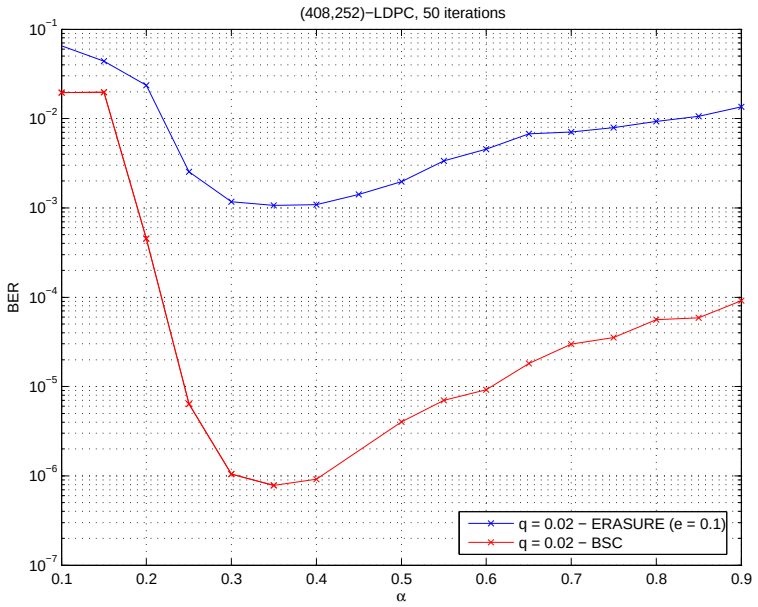


Figure 7.12: BER simulation results for LDPC codes with rate R_c=0.5(n_q= 504, r = 252) and R_c=0.617(n_q= 408, r = 252) obtained with a private quantum channel with erasure

7.3.3 Binary Input Multiple Output Quantum Channel

In this section the performance of a QKD system when employing a private quantum channel modeled as in Figure 7.13 is presented.

In the figures below the most significant results are reported. Figure 7.14, depicts three sets of simulation results. Each pair of curves is associated with a BER and FER simulation results. The LDPC code used for information reconciliation is one with n = 408, r= 252 and code rate R_c = 0.61.

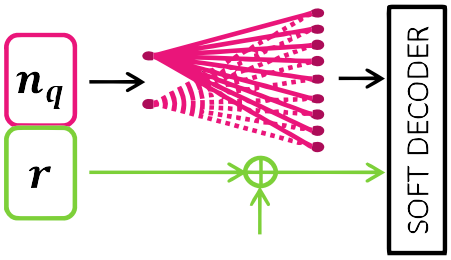


Figure 7.13: The composite channel (composed of the parallel secure and public channels) linking transmitter and receiver in QKD applications

The black pair is for the reference system used for comparison whereby the quantum channel is modeled as an equivalent BSC (i.e., inherently there is no soft metric at the receiver and the only LLR available is from the knowledge of the Q_{BER}). The blue pair represents an idealistic model whereby it has been assumed that the quantum channel did not exist at all and the information transmitted over the quantum channel was presumed to pass through a fictitious AWGN channel with an SNR that would yield the observed Q_{BER} if BPSK was used for data transmission. The red pair represents the core results of this thesis and is associated with the use of soft metrics generated via photon counting as presented earlier in Chapter 5. As is evident from the results there is significant reduction in BER and FER for Q_{BER} values below 0.15 allowing significantly larger portion of the data to be kept during further reconciliation, data sifting and privacy amplification phases of the protocol. For instance at Q_{BER}=0.05, there is more than two orders of magnitude improvement in BER and FER when comparing the proposed soft-metric processing versus the reference protocol whereby the quantum channel is a BSC. To give an idea of potential gains in rate consider that the FER at Q_{BER}=0.1 for the reference system is 0.8, hence, 80% of the blocks have errors and need to be thrown away (a simple mechanism would be to use Cyclic redundancy check (CRC)[1] on each frame to detect the erroneous ones), whereas for the proposed system FER at Q_{BER}=0.1 is 0.07, hence only 7 out of 100 blocks have errors and need to be thrown away.

The estimated Q_{BER} when using the Bayesian estimator is calculated a posteriori based on the number of photons counted at the detection stage which is itself distributed according to the Poisson law:

$$Q_{BER} = E\left[q_n\right] = \sum_{n=0}^{8} q_n p\left(q_n\right) \tag{7.1}$$

[1]The cyclic redundancy check, or CRC, is a technique for detecting errors in digital data, but not for making corrections when errors are detected. It is used primarily in data transmission. In the CRC method, a certain number of check bits, often called a checksum, are appended to the message being transmitted. The receiver can determine whether or not the check bits agree with the data, to ascertain with a certain degree of probability whether or not an error occurred in transmission. If an error occurred, the receiver sends a negative acknowledgement (NAK) back to the sender, requesting that the message be retransmitted.

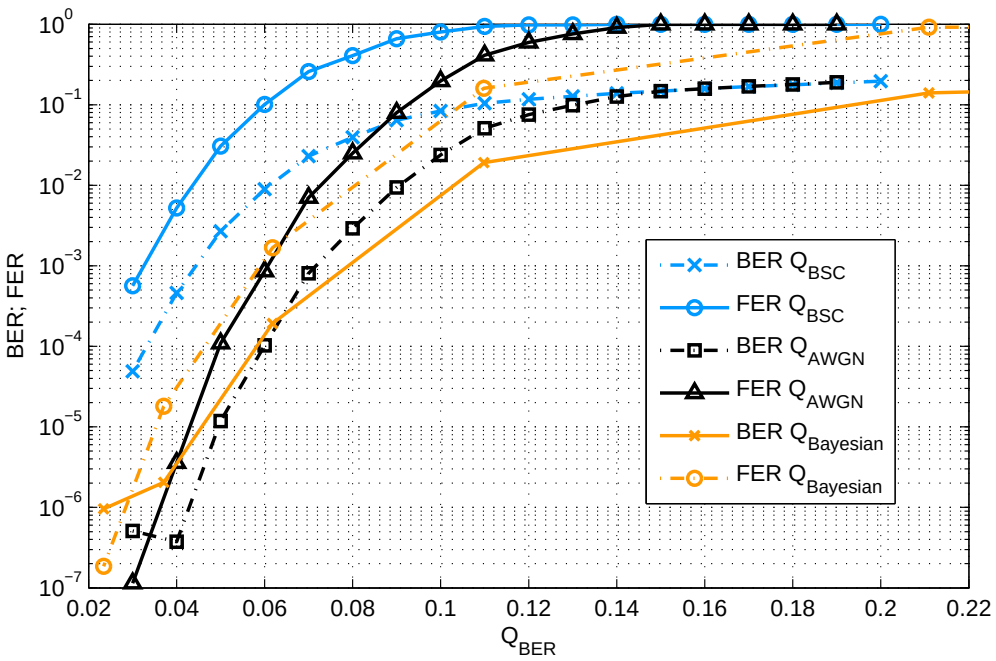


Figure 7.14: BER and FER simulation results for LDPC code with rate R_c=0.617 obtained with the composite scheme of Figure 7.13 and different models for the private quantum channel: BSC (blue curves), AWGN (black curves) and BIMO DMC with Bayesian estimation (orange curves)

where:

$$q_n = \begin{cases} \sum_{k=\frac{n+1}{2}}^{n} \binom{n}{k} pij^k (1-p_{ij})^{n-k} & \text{n odd} \\ \sum_{k=\frac{n}{2}+1}^{n} \binom{n}{k} pij^k (1-p_{ij})^{n-k} + \frac{1}{2}\binom{n}{n/2} pij^{n/2}(1-p_{ij})^{n/2} & \text{n even} \end{cases} \tag{7.2}$$

and $p(q_n) = \frac{e^{-N_c} N_c^n}{n!}$ (Poisson Distribution).

Thus, the number of photons varies for each value of Q_{BER} reported in Figure 7.15 for the case of the BIMO channel with Bayesian estimator, while for the BSC channel Q_{BER} is the transition probability . To highlight this, Figure 9 depicts the mean estimated Q_{BER} as a function of the average number of photons detected per pulse, N_c. Notice that the estimated number of photons N_c can only assume integer values and cannot be too high because this fact would jeopardize the security of the protocol. A smart choice of N_c would help improve the performance of the protocol and would minimize the possible attacks coordinated by Eve.

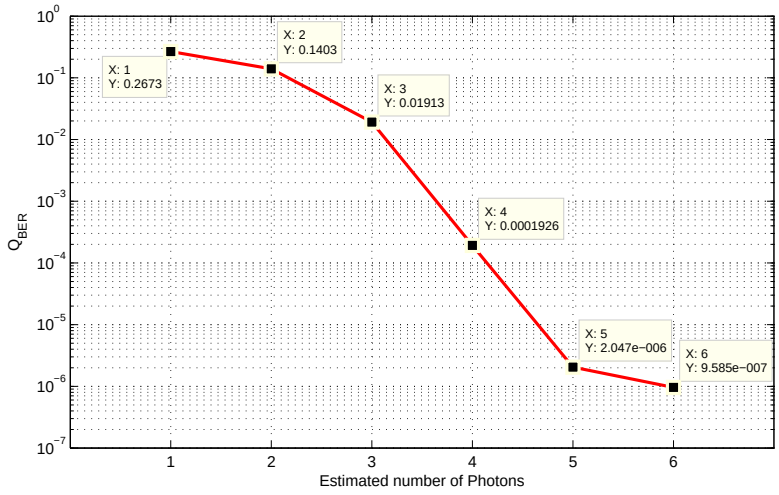


Figure 7.15: Number of estimated photons as a function of the quantum channel BER

Finally, Figure 7.16 depicts the average number of soft decoding iterations and the variance of the number of decoding iterations performed for all three cases discussed above as a function of Q_{BER}. This set of curves provide estimates of decoding complexity and delay in the information reconciliation phase.

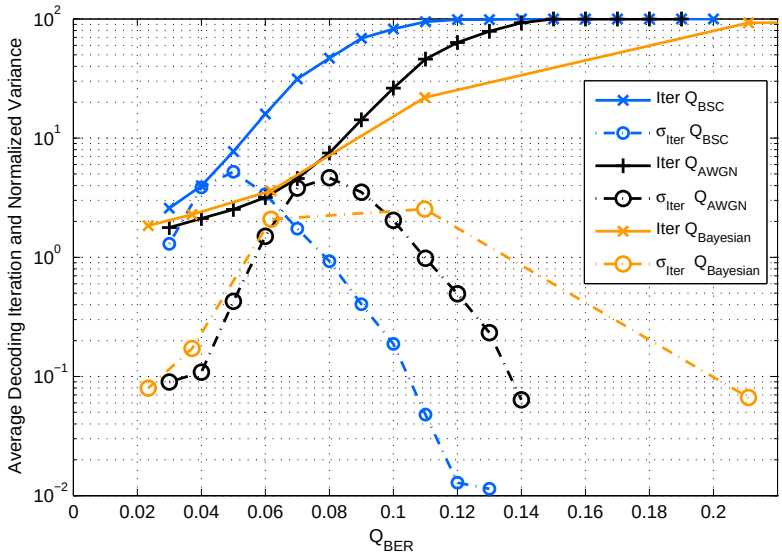


Figure 7.16: Average number of decoding iterations and normalized variance of the number of iterations for the LDPC code with ratesR_c=0.617 as a function of Q for α_Q optimum

7.3.4 Pre-Privacy Amplification: Data Sifting

In Chapter 5 has been established that the availability of soft output information where the decoded bits are paired with the associated reliability offers an instrument for performing efficient and selective pre-data sifting, deleting from the decoded sequence, i.e. the quantum key generated by the FEC procedure, the bits with low reliability, maintaining the most trusted information, and eliminating possible residual errors. Thus, data sifting is performed by comparing the amplitude of the soft metrics associated with the decoded bits, with a threshold T, and sifting only the bits whose reliability values are higher than T. This generates what is known as the partially reconciled key that, while having extremely low number of errors, cannot be guaranteed to be error free.

Figures 7.17 and 7.18 show the residual BER after data sifting as a function of the considered sifting threshold for LDPC codes with $R_c = 0.61$ and R_c=0.5. Plots of this type are intended to be used as design curves, which allow to select correctly the data sifting threshold as a function of the Q_{BER} Q in order to obtain a target residual BER in the partially reconciled key. It has to be noticed that higher values of Q require a higher threshold and a higher number of discarded bits, resulting in a shorter partially reconciled key. From Figures 7.17 and 7.18 it can be noticed that the proposed data sifting technique, while having a negligible cost, can reduce the residual BER by at least two orders of magnitude, largely reducing the number of operations required in the final two-way communication phase. It can also be observed that the residual BER values flatten out for large values of the sifting threshold, so that the incremental gain achievable using very large thresholds tends to zero.

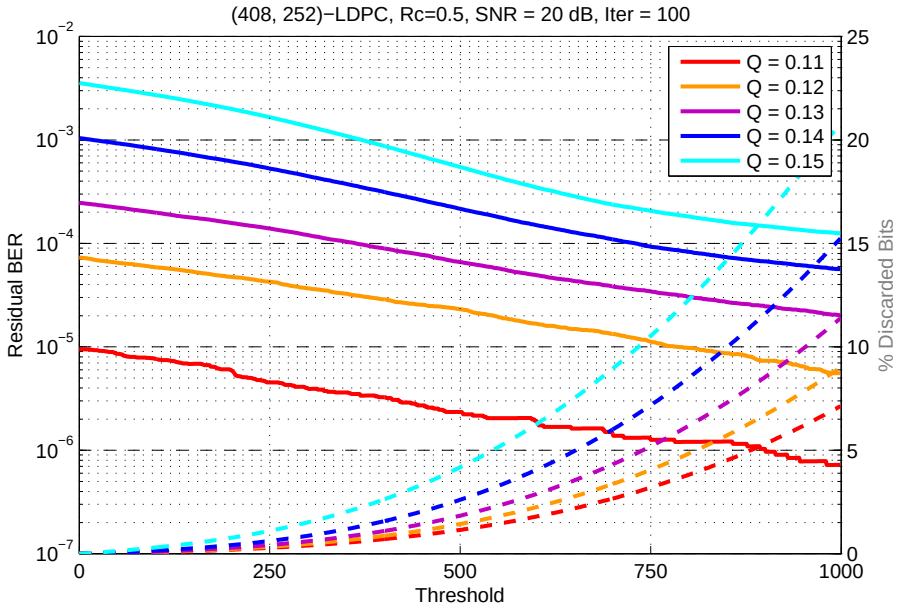


Figure 7.17: Residual BER (solid lines) and percentage of discarded raw-key (dashed lines) during pre-privacy amplification for an LDPC code with n=n_q+r=504, r=252 and R_c=0.5, as a function of the considered threshold for various values of Q

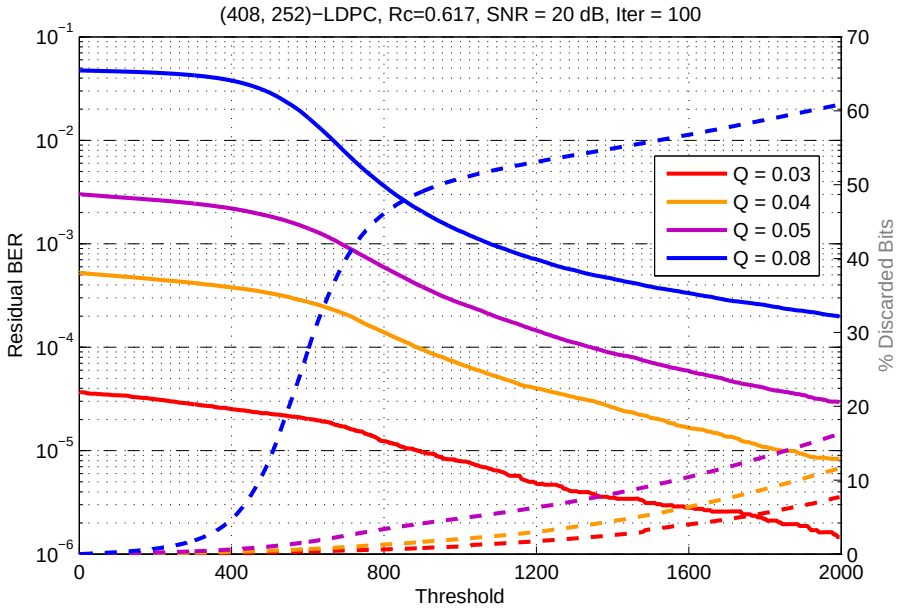


Figure 7.18: Residual BER (solid lines) and percentage of discarded raw-key (dashed lines) during pre-privacy amplification for an LDPC code with n=n_q+r=408, r=252 and R_c=0.61, as a function of the considered threshold for various values of Q

Publications

7.4 Journals

Mondin M., Delgado M., Mesiti F., Daneshgaran F.
"*Soft-processing for Information Reconciliation in QKD Applications*"
International Journal Of Quantum Information, Vol.8, 2010, ISSN:0219-7499.

7.5 Conference proceedings

F. Daneshgaran, M. Delgado, M. Mondin and I. Bari,
"*Classical Capacity of a Bayesian Inference Quantum Channel Employing Photon Counting Detect*"
Proceedings of ISABEL 2011, Barcelona (Spain), Oct. 26-28, 2011, invited paper

---

S. Olivares, M. Delgado and M. Paris
"*On the generation of entanglement from the interference of Gaussian states of light*"
Proceedings of ISABEL 2011, Barcelona (Spain), Oct. 26-28, 2011, invited paper

---

F. Vatta, R. Romano and M. Delgado
"*Turbo codes for Quantum Key Distribution (QKD) applications*"
Proceedings of ISABEL 2011, Barcelona (Spain), Oct. 26-28, 2011, invited paper

---

F. Daneshgaran, M. Delgado and M. Mondin
"*Improved key rates for quantum key distribution employing soft metrics using Bayesian inference with photon counting detectors*"
Proc. SPIE 8163, 81630D (2011); doi:10.1117/12.894330

F. Mesiti, F. Daneshgaran, M. Delgado, M. Mondin
"*Sparse-graph codes for information reconciliation in QKD applications*"
Proceedings of ISABEL 2010, Rome (Italy), Nov. 7-10, 2010, invited paper

---

S. Olivares, M. Paris, M. Delgado, M. Mondin
"*Toward a "Soft" Output Quantum Channel via Bayesian Estimation*"
Proceedings of ISABEL 2010, Rome (Italy), Nov. 7-10, 2010, invited paper

---

M. Mondin, F. Daneshgaran, M. Delgado, F. Mesiti
"*Soft-metric-based information reconciliation techniques for QKD*"
Proc. SPIE 7815, 781502, 2010, SPIE Optics + Photonics 2010 (San Diego, USA) Aug 1-5, 2010, vol. 8, DOI:10.1117/12.858357

M. Mondin, F. Daneshgaran, M. Delgado, F. Mesiti
"*Novel Techniques for Information Reconciliation, Quantum Channel Probing and Link Design for Quantum Key Distribution*"
Proceedings of PSATS 2010, Roma, Italy, February 2010

Conclusions

In any Quantum Key Distribution system, Alice and Bob may use one of two types of reconciliation, in order to preserve the integrity and security of their keys. The first type is interactive reconciliation, which consists of two-way interaction between Alice and Bob over a public classical channel for the detection and correction of errors. The second type of interaction is one-way reconciliation in which a decision is made beforehand regarding how errors are detected and corrected. Considering the fact that, one-way protocols, by their nature, tend to reveal less information over the public channel than interactive protocols where possibly many messages are openly passed back and forth, in this work a novel information reconciliation and data sifting protocol has been proposed, which uses Forward Error Correction (FEC), minimizing the exchange of information related to the secret key that needs to be sent back and forth using the public channel. This protocol, is based on soft decoding of LDPC codes with mixed-metric inputs, where the information derived from a private quantum channel and a classic public channel are jointly used for decoding. The performance of the proposed methods has been studied by simulation, and the effects of the various system parameters have been considered. Furthermore, a feed-forward technique for the identification of a possible eavesdropper has been proposed, based on the behavior (observation of the average number of decoding iterations and its variance) of the LDPC decoder and on the the fact that according to quantum physics, the mere fact of observing a quantum object perturbs it in an irreparable way, so a possible eavesdropper will elevate the bit error rate of the quantum transmission and this will be directly reflected on the performance of the LDPC decoder.

The suggested algorithms can be applied to QKD schemes based both on Single Photon or WLP sources, with or without decoy states. The difference among the different schemes is the use of different channel metrics. However, independently from the scheme used, the protocol allows both parties involved in a quantum key distribution to identify a sifted secret key with minimum information exchange and reduced computational costs.

Specifically, in this thesis, the gains that can be achieved in the secret key rates of a QKD protocol from the use of more advanced receivers employing photon counting detectors have been explored, motivated by the fact that the the presence of such

detectors allows for the generation of soft-metrics at the receiver. Within the context of this system, a multi-level quantum channel *BIMO Quantum-DMC* has been identified and the evaluation of its theoretical capacity bound has been calculated. The BIMO Quantum-DMC offered a capacity improvement over the equivalent BSC quantum channel (leading to a BER improvement when comparing the two channel in presence of an error correction code), translating in a significant reduction of the values of the BER and FER for several Q_{BER} values; meaning that a significant larger portion of the data after the stages of sifting and reconciliation may be kept

There has been much interest in quantum key distribution. Experimentally, quantum key distribution over 150 km of commercial Telecom fibers and over 144 km in atmosphere has been successfully performed. The crucial issues in quantum key distribution are the security and the key rate. All recent experiments are, in principle, insecure due to real-life imperfections. However with the use of methods like decoy states, it is possible to make most of those experiments by using essentially the same set-up. Since the security aspect seems to be *improved* by the use of such methods, it is becoming more and more important to obtain elevated key rates from QKD systems to keep up with the high rates of practically any telecommunication system, this way secure data transmission may be guarantee by using one time pad encryption algorithms.

In general, the availability of the soft-metric allows for the use of advanced iterative soft-decoding techniques during the information reconciliation phase, significantly reducing the residual bit and frame error rates with subsequent impact on the achievable secret key rates which is, as said before, is one of the fundamental performance guideline in QKD. The proposed protocol, while having a negligible cost, can reduce the residual FER in QKD systems, largely reducing the interaction required between the two parties involved, increasing the key rate and protecting the secrecy of the information exchanged

Appendix A

Bra Ket Notation

A.1 Vectors in Euclidean spaces

In physics, basis vectors allow any vector to be represented geometrically using angles and lengths, in different directions, i.e. in terms of the spatial orientations. It is simpler to see the notational equivalences between ordinary notation and bra-ket notation, so for now; consider a vector A as an element of 3-d Euclidean space using the field of real numbers, symbolically stated as $\mathbf{A} \in \mathbb{R}^3$

The vector A can be written using any set of basis vectors and corresponding coordinate system. Informally basis vectors are like building blocks of a vector, they are added together to make a vector, and the coordinates are the number of basis vectors in each direction. Two useful representations of a vector are simply a linear combination of basis vectors, and column matrices. Using the familiar cartesian basis, a vector A is written;

$$\mathbf{A} = A_x\mathbf{e}_x + A_y\mathbf{e}_y + A_z\mathbf{e}_z = \begin{pmatrix} A_x \\ A_y \\ A_z \end{pmatrix}$$

respectively, where e_x, e_y, e_z denotes the cartesian basis vectors (all are orthogonal unit vectors) and Ax, Ay, Az are the corresponding coordinates, in the x, y, z directions. Natural alternatives to Cartesian are spherical and cylindrical systems. In general for any basis in 3d space we write;

$$\mathbf{A} = A_1\mathbf{e}_1 + A_2\mathbf{e}_2 + A_3\mathbf{e}_3 = \begin{pmatrix} A_1 \\ A_2 \\ A_3 \end{pmatrix}$$

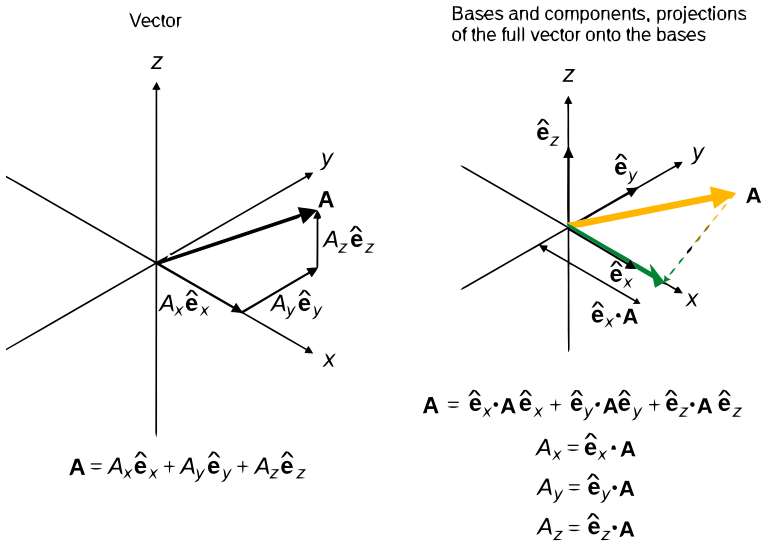


Figure A.1: Cartesian vectors, bases, coordinates and components

Generalizing further, consider a vector A in an N dimensional vector space over the field of complex numbers $\mathbb{C}$, symbolically stated as $\mathbf{A} \in \mathbb{C}^N$. The vector A is still conventionally represented by a linear combination of basis vectors or a column matrix:

$$\mathbf{A} = \sum_{n=1}^{N} A_n \mathbf{e}_n = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_N \end{pmatrix}$$

though the coordinates and vectors are now all complex-valued.

A.2 Bras and kets in Hilbert spaces

Rather than boldtype, over/under-arrows, underscores etc conventionally used elsewhere; $\mathbf{A}, \underline{A}, \vec{A}$, Dirac's notation for a vector uses vertical bars and angular brackets; $|A\rangle$. This applies to all vectors, the resultant vector and the basis. The previous vectors are now written

$$|A\rangle = A_x|e_x\rangle + A_y|e_y\rangle + A_z|e_z\rangle = \begin{pmatrix} A_x \\ A_y \\ A_z \end{pmatrix},$$

$$|A\rangle = A_1|e_1\rangle + A_2|e_2\rangle + A_3|e_3\rangle = \begin{pmatrix} A_1 \\ A_2 \\ A_3 \end{pmatrix},$$

The last one may be written for short by

$$|A\rangle = A_1|1\rangle + A_2|2\rangle + A_3|3\rangle$$

More generally, a vector $|A\rangle$ is an element of a Hilbert space $\mathcal{H}$, meaning $|A\rangle \in \mathcal{H}$, and represented by:

$$|A\rangle = \sum_{n=1}^{N} A_n|e_n\rangle = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_N \end{pmatrix}$$

These vectors are *kets*. For reasons of efficient manipulation, and particularly due to Heisenberg's matrix mechanics, the matrix representation remains. In principle Dirac's notation can be applied universally, though its strict application is to abstract vector spaces - most frequently a projective Hilbert space, denoted $\mathcal{H}$. This space uses the field of complex numbers, again meaning the vector basis and coordinates are complex-valued.

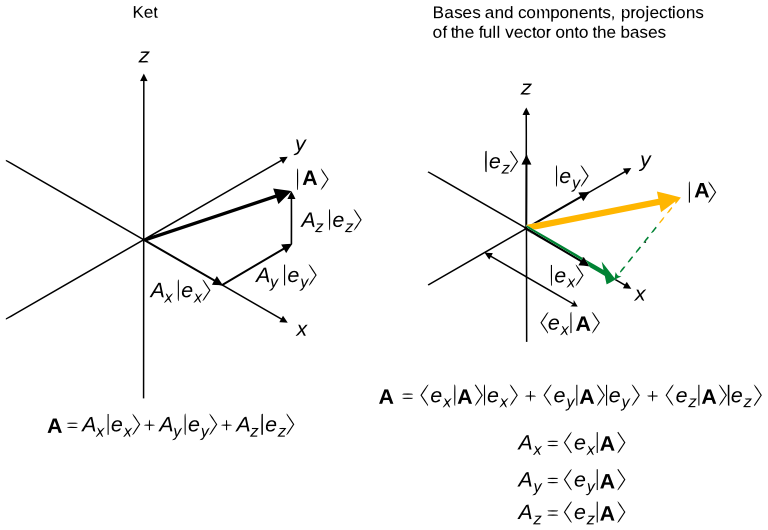


Figure A.2: Ket vectors, bases, coordinates and components

An extra feature not shown above is a dual ket, given by:

$$\langle A| = \sum_{n=1}^{N} A_n^*\langle e_n| = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_N \end{pmatrix}^{*T} = \begin{pmatrix} A_1^* & A_2^* & \cdots & A_N^* \end{pmatrix}$$

These are *bra* vectors.

The bra is simply the conjugate transpose and matrix transpose (taken together the Hermitian conjugate) of the ket and vice versa. The above cases are finite-dimensional Hilbert spaces, i.e. column/row vectors with a finite number of elements. In infinite-dimensional spaces there are infinitely many coordinates and the ket may be written in complex function notation, by prepending it with a bra.

Technically; bras are continuous linear functionals from $\mathcal{H}$ to the complex numbers $\mathbb{C}$, defined by:

$$\langle\psi| : \mathcal{H} \to \mathbb{C}$$

in which the functional takes a ket, and returns a complex number;

$$\langle\psi| \left(|\rho\rangle \right) = \mathrm{IP}\left(|\psi\rangle \, , |\rho\rangle \right),$$

for all kets in the Hilbert space (symbolically $\forall\, |\rho\rangle \in \mathcal{H}$), where IP(,) denotes the inner product defined on the Hilbert space. Here the origin of the bra-ket notation becomes clear: when we drop the parentheses (as is common with linear functionals) and meld the bars together we get $\langle\psi|\rho\rangle$, which is common notation for an inner product in a Hilbert space. This combination of a bra with a ket to form a complex number is called a bra-ket or bracket.

The notation is justified by the Riesz representation theorem, which states that a Hilbert space and its dual space are isometrically conjugate isomorphic. Thus, each bra corresponds to exactly one ket, and vice versa. More precisely, if

$$J : \mathcal{H} \to \mathcal{H}^*$$

is the Riesz isomorphism between $\mathcal{H}$ and its dual space, then

$$\forall \phi \in \mathcal{H} : \ \langle\phi| = J(|\phi\rangle).$$

Note that this only applies to states that are actually vectors in the Hilbert space. Non-normalizable states, such as those whose wavefunctions are Dirac delta functions or infinite plane waves, do not technically belong to the Hilbert space. So if such a state is written as a ket, it will not have a corresponding bra according to the above definition. This problem can be dealt with in either of two ways. First, since all physical quantum states are normalizable, one can carefully avoid non-normalizable states. Alternatively, the underlying theory can be modified and generalized to accommodate such states, as in the GelfandNaimarkSegal construction or rigged Hilbert spaces. In fact, physicists routinely use bra-ket notation for non-normalizable states, taking the second approach either implicitly or explicitly.

A.3 Inner products

In Euclidean space of any finite dimension, the dot product can be defined for vectors using orthonormal bases:

$$\mathbf{a} \cdot \mathbf{B} = \sum_{n=1}^{N} A_n B_n$$

for the same vector, the dot product of a vector with itself is the square of its norm (magnitude)

$$\mathbf{A} \cdot \mathbf{A} = \sum_{n=1}^{N} A_n^2 = \|A\|^2$$

Orthonormality means if two vectors are perpendicular, their dot product is zero, for any two orthonormal basis vectors e_i and e_j this reads,

$$\mathbf{e}_i \cdot \mathbf{e}_j = \delta_{ij}$$

where δ_{ij} is the Kronecker delta.

This operation has the interpretation as a projection of one magnitude of a vector onto the other. Using this fact, the coordinates with respect to the chosen basis are projections of the vector itself to the basis vectors. For the cartesian coordinates they are:

$$A_x = \mathbf{e}_x \cdot \mathbf{A} \quad A_y = \mathbf{e}_y \cdot \mathbf{A} \quad A_z = \mathbf{e}_z \cdot \mathbf{A}$$

For space of finite dimension N, the coordinates are:

$$A_n = \mathbf{e}_n \cdot \mathbf{A}$$

for $n = 1,2,...N$.

Dot products are special cases of the general inner product. In bra-ket notation this is:

$$\langle A|B\rangle = \left(\sum_{n=1}^{N} A_n^* \langle e_n|\right)\left(\sum_{n=1}^{N} B_n |e_n\rangle\right) = \begin{pmatrix} A_1^* & A_2^* & \cdots & A_N^* \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_N \end{pmatrix}$$

For the case of the same vector,

$$\langle A|A\rangle = \left(\sum_{n=1}^{N} A_n^* \langle e_n|\right)\left(\sum_{n=1}^{N} A_n |e_n\rangle\right) = \begin{pmatrix} A_1^* & A_2^* & \cdots & A_N^* \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_N \end{pmatrix} = \sum_{n=1}^{N} |A_n|^2 = \|A\|^2$$

so analogous to the dot product yielding the square of the magnitude of a vector, the inner product of a bra and ket is the square of the vector norm. Again, orthonormality reads,

$$\langle e_i | e_j \rangle = \delta_{ij}$$

Using the inner product on the above euclidean vectors, written in bra-ket notation the cartesian coordinates are

$$A_x = \langle e_x | A \rangle, \quad A_y = \langle e_y | A \rangle, \quad A_z = \langle e_z | A \rangle$$

Appendix B

Operators

B.1 Definitions

Definition 1: An operator $\hat{O}$ is a mathematical entity that transforms a function $f(x)$ into another function $g(x)$ as follows:

$$\hat{O}f(x) = g(x),$$

where f and g are functions of x.

Definition 2: An operator $\hat{O}$ that represents an observable O is obtained by first writing the classical expression of such observable in Cartesian coordinates (e.g., $O = O(x,p)$) and then substituting the coordinate x in such expression by the coordinate operator $\hat{x}$ as well as the momentum p by the momentum operator $\hat{p} = -i\hbar\partial/\partial x$.

Definition 3: An operator $\hat{O}$ is linear if and only if (iff),

$$\hat{O}(af(x) + bg(x)) = a\hat{O}f(x) + b\hat{O}g(x),$$

where a and b are constants.

Definition 4: An operator $\hat{O}$ is hermitian iff,

$$\int \phi_n^*(x)\hat{O}\psi_m(x)dx = \left[\int \psi_m^*(x)\hat{O}\phi_n(x)dx\right]^*,$$

where the asterisk represents the complex conjugate of the expression embraced by brackets.

Definition 5: A function $\phi_n(x)$ is an eigenfunction of $\hat{O}$ iff,

$$\hat{O}\phi_n(x) = O_n\phi_n(x),$$

where O_n is a number called eigenvalue.

B.2 Eigenfunctions and Eigenvalues

An eigenfunction of an operator $\hat{A}$ is a function f such that the application of $\hat{A}$ on f gives f again, times a constant.

$$\hat{A}f = kf$$

where k is a constant called the eigenvalue. It is easy to show that if $\hat{A}$ is a linear operator with an eigenfunction g, then any multiple of g is also an eigenfunction of $\hat{A}$.

When a system is in an eigenstate of observable A (i.e., when the wavefunction is an eigenfunction of the operator $\hat{A}$) then the expectation value of A is the eigenvalue of the wavefunction. Thus if

$$\hat{A}\psi(\mathbf{r}) = a\psi(\mathbf{r})$$

then $< A > = \int \psi^*(\mathbf{r})\hat{A}\psi(\mathbf{r})d\mathbf{r}$ (51) $= \int \psi^*(\mathbf{r})a\psi(\mathbf{r})d\mathbf{r} = a\int \psi^*(\mathbf{r})\psi(\mathbf{r})d\mathbf{r} = a$

assuming that the wavefunction is normalized to 1, as is generally the case. In the event that $\psi(\mathbf{r})$ is not or cannot be normalized (free particle, etc.) then we may use the formula

$$< A >= \frac{\int \psi^*(\mathbf{r})\hat{A}\psi(\mathbf{r})}{d}\mathbf{r}\int \psi^*(\mathbf{r})\psi(\mathbf{r})d\mathbf{r}$$

What if the wavefunction is a combination of eigenstates? Let us assume that we have a wavefunction which is a linear combination of two eigenstates of $\hat{A}$ with eigenvalues a and b.

$$\psi = c_a\psi_a + c_b\psi_b$$

where $\hat{A}\psi_a = a\psi_a$ and $\hat{A}\psi_b = b\psi_b$. Then the expectation value of A is

$$\begin{aligned}
< A > &= \int \psi^*\hat{A}\psi \\
&= \int \left[c_a\psi_a + c_b\psi_b\right]^* \hat{A}\left[c_a\psi_a + c_b\psi_b\right] \\
&= \int \left[c_a\psi_a + c_b\psi_b\right]^* \left[ac_a\psi_a + bc_b\psi_b\right] \\
&= a|c_a|^2\int \psi_a^*\psi_a + bc_a^*c_b\int \psi_a^*\psi_b + ac_b^*c_a\int \psi_b^*\psi_a + b|c_b|^2\int \psi_b^*\psi_b \\
&= a|c_a|^2 + b|c_b|^2
\end{aligned}$$

assuming that ψ_a and ψ_b are orthonormal. Thus the average value of A is a weighted average of eigenvalues, with the weights being the squares of the coefficients of the eigenvectors in the overall wavefunction.

B.3 Hermitian Operator

The expectation value of an operator $\hat{A}$ is given by

$$< A >= \int \psi^*(\mathbf{r})\hat{A}\psi(\mathbf{r})d\mathbf{r}$$

All physical observables are represented by such expectation values. Obviously, the value of a physical observable such as energy or density must be real, so we require $< A >$ to be real. This means that we must have $< A >=< A >^*$, or

$$\int \psi^*(\mathbf{r})\hat{A}\psi(\mathbf{r})d\mathbf{r} = \int (\hat{A}\psi(\mathbf{r}))^*\psi(\mathbf{r})d\mathbf{r}$$

Operators $\hat{A}$ which satisfy this condition are called **Hermitian**. One can also show that for a Hermitian operator,

$$\int \psi_1^*(\mathbf{r})\hat{A}\psi_2(\mathbf{r})d\mathbf{r} = \int (\hat{A}\psi_1(\mathbf{r}))^*\psi_2(\mathbf{r})d\mathbf{r}$$

for any two states ψ_1 and ψ_2.

An important property of Hermitian operators is that their eigenvalues are *real*. We can see this as follows: if we have an eigenfunction of $\hat{A}$ with eigenvalue a, i.e. $\hat{A}\psi_a = a\psi_a$, then for a Hermitian operator $\hat{A}$

$$\begin{aligned} \int \psi_a^*\hat{A}\psi_a &= \int \psi_a(\hat{A}\psi_a)^* \\ a\int \psi_a^*\psi_a &= a^*\int \psi_a\psi_a^* \\ (a-a^*)\int |\psi_a|^2 &= 0 \end{aligned}$$

Since $|\psi_a|^2$ is never negative, we must have either $a = a^*$ or $\psi_a = 0$. Since $\psi_a = 0$ is not an acceptable wavefunction, $a = a^*$, so a is real.

Another important property of Hermitian operators is that their eigenvectors are orthogonal (or can be chosen to be so). Suppose that ψ_a and ψ_b are eigenfunctions of $\hat{A}$ with eigenvalues a and b, with $a \neq b$. If $\hat{A}$ is Hermitian then

$$\int \psi_a^*\hat{A}\psi_b = \int \psi_b(\hat{A}\psi_a)^*$$

$$b \int \psi_a^* \psi_b = a^* \int \psi_b \psi_a^*$$
$$(b - a) \int \psi_a^* \psi_b = 0$$

since $a = a^*$ as shown above. Because we assumed $b \neq a$, we must have $\int \psi_a^* \psi_b = 0$, i.e. ψ_a and ψ_b are orthogonal. Thus we have shown that eigenfunctions of a Hermitian operator with different eigenvalues are orthogonal.

Appendix C

Block codes

Consider a finite set of symbols $\mathbb{F}_q$, called alphabet, with q elements. The information to be processed and the codewords will be expressed with symbols from this alphabet. $\mathbb{F}_q$ has the structure of a (finite) field (in particular the size of the alphabet q is the power of a prime).

Definition 1.1. A linear block code of length n and dimension k is a k-dimensional subspace $\mathcal{C}$ of ${\mathbb{F}_q}^n$ The length of the code fixes the length of the data streams sent through the channel, and the dimension measures the amount of information, without redundancy, that each of these streams has. Encoding is described by means of an encoding map, an injective linear map

$$g : {\mathbb{F}_q}^k \to {\mathbb{F}_q}^n$$

Definition 1.2. A generator matrix of the code is a matrix representation of the encoding map.

Definition 1.3. Let x,$y \in \mathbb{F}^n$. The *Hamming weight* of x is the number of nonzero components of x,$w(x) = \sharp\{i|x_i \neq 0\}$. The *Hamming distance* between x and y is the number of components in which x and y differ, $d(x,y) = \sharp\{i|x_i \neq y_i\}$. The *minimum distance* of a code $\mathcal{C}$ is the minimum Hamming distance between any two different codewords, $d(\mathcal{C}) = min_{x,y\in\mathcal{C}}\{d(x,y)\}$

Because of linearity $d(x,y) = w(x-y)$ and thus $d(\mathcal{C}) = min_{x,y\in\mathcal{C}}\{w(x-y)\} = min_{c\in\mathcal{C}}\{w(c)\}$ Endowed with the Hamming distance, $\mathbb{F}^n$ is a metric space. A block code over $\mathbb{F}^q$ with length n, dimension k and minimum distance d is often referred to as a $[n,k,d]_q$-code. The minimum distance quantifies the number of errors that the code can detect or correct. It is well-known that a code with minimum distance d can detect all errors of weight at most $d-1$ and correct all errors of weight at most $\frac{d-1}{2}$. Therefore the minimum distance of a code characterizes its error correcting capacity.

Appendix D

Quantum Channel Model

In a broad sense, in quantum information theory, a quantum channel is a communication channel which can transmit quantum information, as well as classical information. An example of quantum information is the state of a quantum bit whereas the meaning of classical information is clear.
More formally, since in quantum mechanics observables are associated with Hermitian operators, quantum channels may be viewed as completely positive, trace preserving maps between spaces of operators. In other words, a quantum channel is just a quantum operation viewed not merely as the reduced dynamics of a system but as a pipeline intended to carry quantum information.
Quantum channel is memoryless if the induced mapping at a given time is independent of the past mappings. Quantum channels transmitting quantum information can be viewed as performing a quantum operation mapping two finite dimensional Hilbert spaces.
From the Schrödinger viewpoint, let H_A and H_B be the Hilbert state spaces (finite-dimensional) at the transmit and receiving ends, respectively, of a channel. Let $L(H_A)$ denote the family of operators on H_A. In the Schrödinger picture, a purely quantum channel is a map Φ between density matrices acting on H_A and H_B with the following properties:

1. Since all quantum mechanical operators of interest are linear, Φ needs to be linear.

2. Since density matrices are positive, Φ must preserve the cone of positive elements. In other words, Φ is a positive map.

3. If we couple an ancilla of arbitrary finite dimension n to the system, the induced map on the tensor product $I_n \bigotimes \Phi$, o where I_n is the identity map on the ancilla, must also be positive. Therefore it is required that $I_n \bigotimes \Phi$ is positive for all n. Such maps are called *completely positive*.

4. Density matrices are specified to have trace 1, so Φ has to preserve the trace.

The adjectives **completely positive and trace preserving** used to described a map are sometimes abbreviated **CPTP**. In the literature, sometimes the fourth property is weakened so that Φ is only required to be non trace-increasing. Here, the assumption is that that all channels are CPTP.
From the Heisenberg viewpoint, density matrices acting on H_A only constitute a proper subset of the operators on H_A and same can be said for system B. However, once a linear map Φ between the density matrices is specified, a standard linearity argument, together with the finite dimensional assumption, allow one to extend Φ uniquely to the full space of operators. This leads to the adjoint map Φ^*, which describes the action of Φ in the Heisenberg picture.
Viewing $\Phi : L(H_A) \to L(H_B)$ as a map between Hilbert spaces, we obtain its adjoint Φ^* as:

$$\langle A, \Phi(\rho) \rangle = \langle \Phi^*(A), \rho \rangle$$

While Φ maps states on A to those on B, Φ^* maps observables on system B to observables on system A. This relationship is same as that between the Schrödinger and Heisenberg descriptions of dynamics. The measurement statistics remain unchanged whether the observables are considered fixed while the states undergo operation or vice versa.
It can be directly checked that if Φ is assumed to be trace preserving, Φ^* is unitary, that is $\Phi^*(I) = I$. Physically speaking, this means that, in the Heisenberg picture, the trivial observable remains trivial after applying the channel.
In the context of transmitting quantum bits through either a fiber optics channel or free space, the above broad generalizations and definitions of the quantum channel are of little use. In practical applications to QKD, it is of importance to understand what happens to the q-bit as it traverses the channel. Since the q-bit is often associated with transmission of photons, it is important to characterize what happens to photons as they traverse the channel.
The most used quantum channel is called depolarizing channel and it is described by the unitary transformation:

$$\varepsilon(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

whereby X, Z, and Y are ordinary Pauli matrices describing, respectively, a bit flip, a phase flip, and a combination of bit and phase flips. The depolarizing channel transmits independently each quantum bit described by the density operator ρ, identifying a mixed-state quantum bit. The quantum bit is transmitted correctly with probability $(1-p)$, while it is bit flipped, phase flipped or both independently with probability $\frac{p}{3}$. Such a channel can be simulated by using a 4-ary channel with probabilities (with A=1):

$$p_X = \frac{p}{A+2}$$

$$p_Y = \frac{p}{A+2}$$

$$p_Z = \frac{pA}{A+2}$$

or a cascade of two dependent classical Binary Symmetric Channels (BSC) with probabilities of errors, respectively, p_X and p_Z. The first BSC models a bit flip with probability p_X, while the second BSC a phase flip with probability p_Z. However, a reasonable approximation is to consider statistical independence among the cascaded BSCs so that the cascade is equivalent to a unique BSC with cross-over probability Q that can be related to p_X and p_Z as follows:

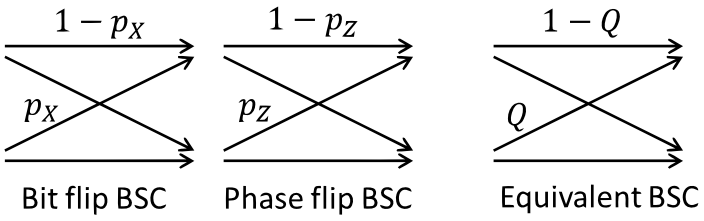


Figure D.1: Quantum channel model as the cascade of two BSC

Given that:

$$p_X = p_Y = p_Z = p/3$$

We have:

$$Q = \frac{3p_X}{2} = \frac{3p_Z}{2}$$

The latter follows from the conditions which make both models equivalent to each other:

$$1 - Q = (1 - p_X)(1 - p_Z)$$

$$Q/3 = p_X\,(1 - p_Z) = p_Z\,(1 - p_X) = p_X p_Z$$

These equations signify the fact that a bit or phase flip occur with probability $2Q/3$, where Q is the chosen quantum cross-over probability of the quantum BSC channel. The classic public channel uses classic communication schemes, and possibly very strong coding for data protection, so that the bit error rate of the classic channel is generally extremely low. Additive White Gaussian Noise (AWGN) is generally the predominant impairment on the classic channel, so that the equivalent channel model is as shown below:
In this model, Xrk is the k-th transmitted symbol, $Nk \sim N(0, \sigma 2)$ is a Gaussian random variable with zero mean and variance $\sigma 2 = N_0/2 = Eb/(2\eta_s)$, where $\eta_s = E_b/N_0$ is the wireless link signal-to-noise ratio, and Yrk is the real sample obtained at the output of the public channel detector.

Bibliography

[1] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, "Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography," *Japanese Journal of Applied Physics*, vol. 43, no. No. 9A/B, p. 10, 2004.

[2] T. Schmitt-Manderbach, H. Weier, M. Frst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. Rarity, and et al., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, pp. 1–4, 2007.

[3] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, and et al., "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, 2007.

[4] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[5] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005.

[6] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of the American Institute of Electrical Engineers*, vol. XLV, no. 55, pp. 295–301, 1926.

[7] C. E. Shannon, "Communication theory of secrecy systems," *MD computing computers in medical practice*, vol. 28, no. 1, pp. 656–715, 1949.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[10] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, vol. 35, pp. 124–134, 1994.

[11] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance.," *Nature*, vol. 414, no. 6866, pp. 883–887, 2001.

[12] P. A. M. Dirac, "A new notation for quantum mechanics," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 35, no. 03, p. 416, 1939.

[13] G. E. Moore, "Lithography and the future of moore's law," *Proceedings of SPIE*, vol. 2437, no. May, pp. 2–17, 1995.

[14] W. Heisenberg, "Ber quantentheoretische umdeutung kinematischer und mechanischer beziehungen (the actual content of quantum theoretical kinematics and mechanics).," *Zeitschrift Fr Physik*, vol. 33, no. 1, pp. 879–893, 1925.

[15] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[16] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[17] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, vol. 175, pp. 175–179. Bangalore, India, 1984.

[18] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information*. No. ISBN: 978-3-540-66778-0, Springer, 2000.

[19] H.-K. Lo, T. Spiller, and S. Popescu, *Introduction to Quantum Computation and Information*, vol. 399. World Scientific, 1998.

[20] N. Ilic, "The ekert protocol," *Quantum*, 1991.

[21] M. L. Bellac, *A Short Introduction to Quantum Information and Quantum Computation*, vol. 60. Cambridge University Press, 2006.

[22] V. Scarani, *Quantum Physics A First Encounter: Interference,Entanglement, and Reality*. Oxford: Oxford Univ. Press, 2006.

[23] M. Dusek, N. Lutkenhaus, and M. Hendrych, "Quantum cryptography," *Progress in Optics*, vol. 18, no. 8, p. 51, 2006.

[24] H.-K. Lo and Y. Zhao, "Quantum cryptography," *Encyclopedia of Complexity and Systems Science*, vol. 8, p. 7265, 2009.

[25] A. Nakassis, "Expeditious reconciliation for practical quantum key distribution," *Proceedings of SPIE*, vol. 5436, pp. 28–35, 2004.

[26] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," *Advances*, vol. 765, pp. 410–423, 1994.

[27] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[28] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. July 1928, pp. 379–423, 1948.

[29] M. J. E. Golay, "Notes on digital coding," *Proceedings of the IRE*, vol. 37, no. 6, p. 657, 1949.

[30] P. Elias, "Coding for noisy channels," *IRE National Convention Record*, vol. 3, no. 4, pp. 37–47, 1955.

[31] E. R. Berlekamp, R. J. McEliece, and H. C. A. Van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[32] R. G. Gallager, "Low-density parity-check codes," *Information Theory IRE Transactions on*, vol. 8, no. 1, pp. 21–28, 1962.

[33] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[34] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," 2001.

[35] K. V. Price, R. M. Storn, J. A. Lampinen, A. Shokrollahi, and R. Storn, "Design of efficient erasure codes with differential evolution," in *Differential Evolution*, Natural Computing Series, pp. 413–427, Springer Berlin Heidelberg, 2005.

[36] D. Elkouss, A. Leverrier, R. Allaume, and J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," *2009 IEEE International Symposium on Information Theory*, no. 1, pp. 1879–1883, 2009.

[37] R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, 1981.

[38] X. Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," 2005.

[39] L.-d. P.-c. Codes, T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 619–637, 2001.

[40] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[41] F. Vatta, R. Romano, and F. Mesiti, *Analysis and design of parallel concatenated channel codes for Quantum Key Distribution (QKD) applications*. IEEE, 2010.

[42] G. Brassard, N. Lutkenhaus, T. Mor, and B. Sanders, "Limitations on practical quantum cryptography," *Physical Review Letters*, vol. 85, no. 6, pp. 1330–3, 2000.

[43] R. J. Glauber, "Coherent and incoherent states of the radiation field," *Physical Review*, vol. 131, no. 6, pp. 2766–2788, 1963.

[44] O. S. et alii, "Toward a soft output quantum channel via bayesian estimation," *Proceedings of ISABEL*, Nov 2010. Rome, Italy.

[45] D. Brivio, S. Cialdi, S. Vezzoli, B. Teklu, M. G. Genoni, S. Olivares, and M. G. A. Paris, "Experimental estimation of one-parameter qubit gates in the presence of phase diffusion," *Physical Review A*, vol. 81, no. 1, pp. 1–7, 2009.

[46] R. D. Gill, "Conciliation of bayes and pointwise quantum state estimation: Asymptotic information bounds in quantum statistics," *math0512443*, pp. 239–261, 2005.

[47] B. Teklu, S. Olivares, and M. G. A. Paris, "Bayesian estimation of one-parameter qubit gates," *Journal of Physics B Atomic Molecular and Optical Physics*, vol. 42, no. 3, p. 10, 2008.